CHAPMAN LAW REVIEW

Citation: Michelle Norris, *"Senator . . . I'm Singaporean!": Privacy Regulation and Data Transfers in Cross-Border Corporations*, 28 CHAP. L. REV. 141 (2025).

"Senator . . . I'm Singaporean!": Privacy Regulation and Data Transfers in Cross-Border Corporations

Michelle Norris

CONTENTS

I. INTRODUCTION 143
II. BACKGROUND 148
A. Privacy Laws and Data Transfers 148
B. The Basics of Cross-Border Data Transfers 151
III. THE CURRENT STATE OF PRIVACY LAWS AFFECTING TIKTOK'S DATA STORAGE AND TRANSFER: A BRIEF OVERVIEW 153
A. Current State of Privacy Laws in China 155
B. Current State of Privacy Laws in Malaysia 159
C. Current State of Privacy Laws in Texas 161
D. Current State of Privacy Laws in Singapore 163
E. Potential U.S. Federal Privacy Law 165
IV. *SCHREMS* AND CPEA: CURRENT U.S. CROSS-BORDER DATA TRANSFER POLICIES 166
A. *Schrems* Decisions and U.S.-EU Privacy Shield 167
B. APEC's CPEA 171
C. TikTok's Data Structure: Data Storage, Transfer, and Usage Practices 172
V. CONFLICT OF LAWS: PROPOSED SOLUTION FOR SAFE AND EFFICIENT DATA STORAGE AND TRANSFERS IN THE AGE OF CLOUD COMPUTING 177
A. USMCA as a Basis for a Multilateral Cross-Border Data Transfer Provision 178
B. Likelihood of Adoption and the Future of Cross-Border Data Governance 181
VI. CONCLUSION 182

"Senator . . . I'm Singaporean!": Privacy Regulation and Data Transfers in Cross-Border Corporations

*Michelle Norris**

A recent congressional hearing involving social media companies, including TikTok and Facebook, made headlines when Senator Tom Cotton of Arkansas grilled the TikTok CEO, Shou Zi Chew, repeatedly asking him if he had ties to China or its Communist Party. The Singaporean CEO, who has served as TikTok's CEO since 2021, repeatedly replied, "Senator . . . I'm Singaporean!" While Senator Cotton, evoking McCarthy-era sentiments, was severely criticized for his racism and what appears to be a lack of understanding about corporate governance, another problem emerged.

TikTok, which is a subsidiary of the Chinese-owned ByteDance, operates in countries around the world and stores its data in Malaysia, Singapore, and the United States. In today's global privacy landscape, each of these countries has differing privacy laws that, at times, conflict regarding how to handle and transfer data. The lack of consensus on how to store and transfer consumer data exposes corporations to the potential risk of hacking if proper oversight and precautions are not followed.

Accordingly, with data becoming a new global currency for expanding businesses, governments must work together to find a solution that streamlines the handling, storage, and transfer of data. Using the United States-Mexico-Canada Agreement as a baseline to create a cross-border data transfer treaty, this Article proposes a multilateral agreement akin to the General Data Protection Regulation to protect consumer data and remove confusion about conflicts of law.

---

* Juris Doctor, California Western School of Law, April 2024; Editor-in-Chief, *California Western Law Review*, 2023–2024; B.A. in English Literature and Creative Writing, Miami University, 2014. The author would like to give thanks to Justine Phillips for her continued mentorship. The author would also like to give special thanks to her husband, family, and friends for their love, support, and patience while writing this Article; she could not have accomplished this milestone without their unwavering encouragement. The views expressed herein are the author's own, and do not necessarily reflect the views or opinions of her employer.

I. INTRODUCTION

On February 1, 2024, Senator Tom Cotton of Arkansas made headlines when he questioned Shou Zi Chew, the Chief Executive Officer (CEO) of the social media corporation, TikTok.[1] The congressional hearing was notable for multiple reasons, one being Senator Cotton's purported misunderstanding regarding Chew's national origin.[2] But while the hearing exposed a clear misunderstanding of the corporate structure of TikTok, as well as the national origin of its CEO, the underlying issue was actually, "Where is the data?" With a twenty percent increase in cyberattacks from 2022 to 2023,[3] paranoia surrounding the use and transfer of data is growing.

The staggering increase in cyberattacks was also accompanied by an increase in victims: the number of individuals whose data was stolen doubled from 2022 to 2023.[4] According to one study, the increase in cyberattacks is likely caused by three things: (1) cloud misconfiguration, (2) new types of ransomware attacks, and (3) increased exploitation of vendor systems.[5] The increased number of attacks is quite troubling given that "people are now living more of their lives online, meaning that corporations, governments, and other types of organizations collect more and more personal data—sometimes with little choice from individuals."[6] Since this personal data is more

---

1 *See, e.g.*, Diba Mohtasham, *Tom Cotton Grills Singaporean TikTok CEO: Are You a Chinese Communist?*, NPR (Feb. 1, 2024, 2:07 PM), https://www.npr.org/2024/02/01/1228383578/tom-cotton-tiktok-ceo-singapore-china [https://perma.cc/7KPW-43HU].

2 *See id.* Senator Cotton's interrogation of Chew, recently revisited in an episode of HBO's *Last Week Tonight with John Oliver*, culminated in the question, "Have you ever been a member of the Chinese Communist Party?" LastWeekTonight, *TikTok Ban: Last Week Tonight with John Oliver (HBO)*, YOUTUBE, at 18:17 (Nov. 21, 2024), https://www.youtube.com/watch?v=5CZNlaeZAtw [https://perma.cc/U3WN-LZEB]. An incredulous Chew responded, "Senator, I'm Singaporean, no." *Id.* at 18:20. Cotton retorted, "Have you ever been associated or affiliated with the Chinese Communist Party?" *Id.* at 18:22. Chew calmly reiterated, "No, Senator. Again, I'm Singaporean." *Id.* at 18:25.

3 Stuart Madnick, *Why Data Breaches Spiked in 2023*, HARV. BUS. REV. (Feb. 19. 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 [https://perma.cc/37E9-RRU8].

4 *Id.*

5 *Id.* (citing STUART E. MADNICK, THE CONTINUED THREAT TO PERSONAL DATA: KEY FACTORS BEHIND THE 2023 INCREASE 2, 8 (2023)).

6 MADNICK, *supra* note 3, at 2.

commonly being used for profitable ventures, it is increasingly of value to cybercriminals.[7]

With today's massive increase in data generation, the number of potential targets for cyberattacks has grown exponentially. In 2018, the world produced 33 zettabytes[8] of data each day—a figure that is accelerating rapidly with the creation of the Internet of Things.[9] Today, it is estimated that 147 zettabytes of data are created each day.[10] It is further estimated that 181 zettabytes of data will be generated in 2025.[11]

Adding to the increased paranoia is general confusion surrounding privacy laws. Currently, there is no federal privacy law. While a proposed bipartisan bill[12] may change the lack of a federal standard governing data privacy, previous efforts to pass a federal privacy law were unsuccessful, leading some experts to believe this bill will meet the same fate.[13] Nevertheless, nineteen

---

7 *See id.*

8 A zettabyte is equal to 1,000,000,000,000,000,000,000 bytes. *Zettabyte – The Storage Capacity Unit Explained*, IONOS (Sept. 13, 2021) https://www.ionos.com/digitalguide/websites/web-development/what-is-a-zettabyte/ [https://perma.cc/AVQ2-UF2X].

9 Mwalimu Phiri, *Exponential Growth of Data*, MEDIUM (Nov. 19, 2022), https://medium.com/@mwaliph/exponential-growth-of-data-2f53df89124 [https://perma.cc/ML2J-TTLA]; *see also* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/ [https://perma.cc/A6GN-F5YS] (Dec. 10, 2021, 8:30 AM) (explaining how the "Internet of Things," a growing network of interconnected smart devices, is driving the exponential growth of data).

10 Fabio Duarte, *Amount of Data Created Daily (2024)*, EXPLODING TOPICS (June 13, 2024), https://explodingtopics.com/blog/data-generated-per-day [https://perma.cc/8JWZ-CMSP].

11 *Id.*

12 *Committee Chairs Rodgers, Cantwell Unveil Historic Draft Comprehensive Data Privacy Legislation*, ENERGY & COM. CHAIR RODGERS (Apr. 7, 2024), https://energycommerce.house.gov/posts/committee-chairs-rodgers-cantwell-unveil-historic-draft-comprehensive-data-privacy-legislation [https://perma.cc/8KA5-FH6K] (describing some of the major rights in the proposed bill); *see also* Rebecca Klar, *5 Things to Know About the Bipartisan Data Privacy Bill*, THE HILL (Apr. 9, 2024, 6:00 AM), https://thehill.com/policy/technology/4581269-5-things-to-know-about-the-bipartisan-data-privacy-bill/ [https://perma.cc/Q9SX-B4GT].

13 Jedediah Bracy, *Stakeholders React to Draft American Privacy Rights Act*, IAPP (Apr. 9, 2024), https://iapp.org/news/a/stakeholders-react-to-draft-american-privacy-rights-act/ [https://perma.cc/6H3C-9MWX]. *But see* Thomas Claburn, *US Legislators Propose American Privacy Rights Act – and it Looks Quite Good*, THE REGISTER (Apr. 9, 2024, 1:32 PM), https://www.theregister.com/2024/04/09/us_federal_privacy_law_apra/ [https://perma.cc/ZG2T-SFYC] (arguing that this latest version of a federal privacy act is better than previous iterations and has a greater potential to pass).

states have passed comprehensive privacy laws, and four more state legislatures are currently considering similar proposals.[14] Each of these laws is unique, with some offering greater protections[15] (like those of California[16] and Colorado[17]) and others that are narrowly written to cover only health data (like those of Washington[18]) or the use of data by social media companies with over one billion dollars in gross annual revenue (like that of Florida).[19]

Comparable to the divide between state privacy laws is the disconnect between international privacy laws.[20] While similar to California and Colorado,[21] the European Union (EU) has its own set of privacy laws: the General Data Protection Regulation (GDPR).[22] The GDPR covers all twenty-seven member

---

14 *See* Andrew Folks, *U.S. State Privacy Law Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/K9ZV-WL22] (July 22, 2024).

15 See generally *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L. (Mar. 18, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/ [https://perma.cc/NN5G-UBT3], for a discussion on the protections of passed comprehensive privacy laws as of March 2024.

16 The first California privacy law passed by the state legislature was the California Consumer Privacy Act (CCPA). California Consumer Privacy Act of 2018, 2018 Cal. Stat. 1807 (codified as amended at CAL. CIV. CODE §§ 1798.100–.199). This Act was amended by the California Privacy Rights Act and supplemented by the CCPA Regulations, which are passed through an informal rulemaking procedure by the California Privacy Protection Agency. California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Proposition 24 (West) (codified at CAL. CIV. CODE §§ 1798.100—.199.100) [hereinafter CPRA]; California Consumer Privacy Act Regulations, CAL. CODE REGS. tit. 11, §§ 7000–7304 (2024).

17 *See, e.g.*, COLO. REV. STAT. ANN. § 6-1-713.5 (West 2024); Colorado Privacy Act, COLO. REV. STAT. ANN. §§ 6-1-1305 to -1313 (West 2024). While discussion about the Colorado Privacy Act is outside the scope of this Article, for more specific information on this Act, see Sarah Rippy, *Colorado Privacy Act Becomes Law*, IAPP (July 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law/ [https://perma.cc/CJ4Y-BVG6].

18 Washington My Health, My Data Act, WASH. REV. CODE § 19.373 (2024).

19 Florida Digital Bill of Rights, FLA. STAT. § 501.702(9)(a)(5) (2024).

20 *See Data Protection and Privacy Legislation Worldwide*, UN TRADE & DEV., https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [https://perma.cc/XLV5-VSP9] (last visited Mar. 3, 2024) (explaining that 71% of countries have legislation, 9% have draft legislation, 15% have no legislation, and the remaining 5% of countries lack data).

21 *See* Richard Lawne, *GDPR vs U.S. State Privacy Laws: How Do They Measure Up?*, FIELDFISHER (Jan. 3, 2023), https://www.fieldfisher.com/en/insights/gdpr-vs-u-s-state-privacy-laws-how-do-they-measure [https://perma.cc/QK2F-L7WQ].

22 *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]. For a discussion on the history of GDPR, see generally *The History of the General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR, https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [https://perma.cc/7AXD-GV3X] (last visited Mar. 3, 2024).

countries,[23] with countries like the United Kingdom (UK) (which is no longer a part of the EU) de facto adopting GDPR through similar resolutions.[24] With the myriad of international laws passed every day, determining which laws to apply to cross-border corporations engaged in data transfers is becoming increasingly complex. The lack of clarity leaves corporations without a clear set of rules to follow: "Varying jurisdictional regulations are stipulating different levels of personal and business data [to] be stored domestically to incongruent degrees, leaving much ambiguity and uncertainty around legal transfers to and from certain countries."[25]

An example of this complexity has appeared in the case of TikTok. ByteDance, a Chinese corporation that owns TikTok,[26] houses its user data in three places: Malaysia, Singapore, and the United States.[27] All three of these countries currently have contradictory data transfer laws. Using TikTok as an anchor for discussion on conflicting data privacy laws, this Article proposes a solution for (1) corporations dealing with cross-border data transfers when their physical repositories are in different locations, and (2) nations attempting to streamline extraterritorial data transfers. This Article critically analyzes the shortcomings in cross-border data transfer privacy laws and proposes a legal solution to the conflicting laws. Using the United States-Mexico-Canada Agreement (USMCA) (which substitutes

---

23 *EEA & UK General Data Protection Regulation (GDPR)*, ACCESS TUFTS, https://access.tufts.edu/eea-uk-general-data-protection-regulation-gdpr [https://perma.cc/9835-4P55] (last visited Mar. 3, 2024). GDPR also applies to all countries in the European Economic Area, such as Iceland, Norway, and Lichtenstein. *Id.*

24 *The Data Protection Act*, GOV.UK, https://www.gov.uk/data-protection [https://perma.cc/73Y7-JYBS] (last visited Mar. 3, 2024). The UK voted to leave the EU in 2016, officially executing the break in 2021. *See Brexit: What You Need to Know About the UK Leaving the EU*, BBC (Dec. 30, 2020), https://www.bbc.com/news/uk-politics-32810887 [https://perma.cc/MV6S-B5X8]. For a discussion on issues and drawbacks of the UK leaving the EU, see generally Michelle R. Norris, *Activating Anti-Trust Pinch Points*: *Microsoft's Activision Merger Conundrum and International Irregularities in Anti-Trust Law*, 12 LOY. U. CHI. J. REGUL. COMPLIANCE 90 (2024).

25 Alex LaCasse, *IAPP GPS 2024: Localization, Adequacy Define Current Data Transfer Landscape*, IAPP (Apr. 4, 2024), https://iapp.org/news/a/iapp-gps-diverging-data-localization-laws-complicate-future-of-crossborder-dataflows/ [https://perma.cc/H7P7-FZ3L].

26 *See Who Owns TikTok's Parent Company, ByteDance?*, TIKTOK: U.S. DATA SEC. [hereinafter *Who Owns TikTok?*], https://usds.tiktok.com/who-owns-tiktoks-parent-company-bytedance/ [https://perma.cc/2BAP-PJRQ] (last visited Apr. 10, 2024).

27 *The Truth About TikTok: Separating Fact from Fiction*, TIKTOK (Apr. 16, 2023), https://newsroom.tiktok.com/en-au/the-truth-about-tiktok [https://perma.cc/CD4V-5JF5].

the North America Free Trade Agreement (NAFTA)[28] as a baseline, this Article proposes a multilateral privacy treaty akin to the GDPR to protect consumer data and remove confusion over conflicts of law.

In Part II, this Article gives the necessary background to understand and appreciate the conflicting laws that govern data transfers, focusing on those countries and the U.S. states where TikTok stores its data. Part III discusses TikTok's data storage, usage, and transfer practices, made all the more imperative by the looming ban or sale of TikTok to be completed by January 19, 2025.[29] The legislation mandating the ban or sale was upheld by the U.S. Court of Appeals for the District of Columbia Circuit on December 6, 2024, and its fate now rests with the Supreme Court, which will hear oral arguments on January 10, 2025.[30] Part IV concludes by analyzing two possible solutions to

---

28 *See* United States-Mexico-Canada Agreement Implementation Act, Pub. L. No. 116-113, 134 Stat. 11 (2020) (replacing Canada-Mexico-United States: North American Free Trade Agreement, Dec. 17, 1992, 32 I.L.M. 289).

29 *See* Lukas I. Alpert, *Trump's Shifting Stance on TikTok Ban Signals a Regulatory Roller Coaster in Second Term*, MARKETWATCH (Nov. 22, 2024, 8:58 AM), https://www.marketwatch.com/story/trumps-shifting-stance-on-tiktok-ban-signals-a-regulatory-roller-coaster-in-second-term-66c2b210 [https://perma.cc/PLA3-WRBA]. At present, the future of TikTok is unclear:

> The fate of TikTok in the U.S. has been up in the air since 2020, when then-President Trump moved to ban the popular video app because of national security concerns. That set off four years of back-and-forth between the app's Chinese owners and the U.S. government, with a possible ban scheduled to go into effect one day before Trump's inauguration in January. One hitch: Trump recently changed his mind, joining TikTok in June and posting on social media, "Those who want to save TikTok in America, vote for Trump."

Wendy Lee & Andrea Chang, *Trump Wanted to Ban TikTok. Will His Return to Office Help Save It?*, L.A. TIMES (Nov. 22, 2024, 3:00 AM), https://www.latimes.com/entertainment-arts/business/story/2024-11-22/donald-trump-bytedance-tiktok-biden [https://perma.cc/863Y-TUR6].

30 *See* Alison Durkee, *Court Refuses to Pause TikTok Ban as Case Heads to Supreme Court*, FORBES (Dec. 13, 2024, 8:09 PM), https://www.forbes.com/sites/alisondurkee/2024/12/13/court-refuses-to-pause-tiktok-ban-as-case-heads-to-supreme-court/ [https://perma.cc/84L5-SAGD] ("The U.S. Court of Appeals for the D.C. Circuit declined to pause its ruling upholding the federal government's law requiring TikTok to divest from Chinese parent company ByteDance or else be banned from U.S. app stores, after TikTok asked for the court to halt the ruling while the company requested the Supreme Court to take up the case."); David Shepardson & Mike Scarcella, *US Appeals Court Upholds TikTok Law Forcing Its Sale*, REUTERS (Dec. 6, 2024, 4:23 PM) https://www.reuters.com/legal/us-appeals-court-upholds-tiktok-law-forcing-its-sale-2024-12-06/ [https://perma.cc/2MD2-5ZQL] ("The decision is a major win for the Justice Department and opponents of the Chinese-owned app and a devastating blow to TikTok parent ByteDance. It significantly raises the prospects of an unprecedented

the current lack of clarity surrounding which privacy laws govern. This section proposes a two-part solution: first, implementing a GDPR *Schrems II*-like provision mitigating risk with cross-border data transfers, and second, a choice-of-law clause to include in TikTok's Terms & Conditions to provide more clarity for users.

II. BACKGROUND

A. Privacy Laws and Data Transfers

To fully understand and appreciate both the risks of data transfers, as well as the need for specific legislation, the governing privacy laws of each location must be discussed in turn. In Section II.A, this Article briefly outlines laws (or the lack thereof) surrounding data transfers, using GDPR as an anchor for discussion. Since TikTok stores its data in three distinct geographical locations (Malaysia, Singapore, and the United States)[31] and is a wholly-owned subsidiary of ByteDance (a Chinese corporation),[32] all four jurisdictions' privacy laws must be discussed to understand their implications regarding conflicts of laws.

---

ban in just six weeks on a social media app used by 170 million Americans."); *see also* Mark Sherman, *Supreme Court Will Hear Arguments over the Law that Could Ban TikTok in the US if It's Not Sold*, ASSOCIATED PRESS (Dec. 18, 2024, 11:43 AM), https://apnews.com/article/supreme-court-tiktok-china-us-ban-08d6fffdcd2dde5100fcdf8a452dd5cc [https://perma.cc/94JU-A4TB].

31 Per TikTok's website, "all new U.S. user data is stored automatically in Oracle's U.S. Cloud infrastructure, and access is managed exclusively by the TikTok US Data Security team." *TikTok Facts: How We Secure Personal Information and Store Data*, TIKTOK (Oct. 12, 2023), https://newsroom.tiktok.com/en-us/tiktok-facts-how-we-secure-personal-information-and-store-data [https://perma.cc/964B-H4MS] (explaining TikTok's data collection and storage practices generally).

32 Dan Primack, *Shotgun Divorce: How ByteDance Could Save TikTok from a U.S. Ban*, AXIOS (Mar. 11, 2024), https://www.axios.com/2024/03/11/tiktok-us-ban-bytedance-divest-sell [https://perma.cc/27SJ-L34H]. While ByteDance owns 100% of TikTok, it is important to note that 60% of ByteDance is owned by outside investors, with the remaining 40% owned by ByteDance itself and global employees. *Id.* While the TikTok forced sale dispute will be referenced throughout this Article, an in-depth discussion on the corporate ownership and divestiture proposal is outside the scope of this Article. For a more in-depth discussion of ByteDance and TikTok's corporate structures, see *TikTok Is Not the Only Chinese App Thriving in America*, THE ECONOMIST (Mar. 21, 2024), https://www.economist.com/business/2024/03/21/tiktok-is-not-the-only-chinese-app-thriving-in-america [https://perma.cc/H5CD-5UAY]; Anupam Chander, *Trump v. TikTok*, 55 VAND. J. TRANSNAT'L L. 1145, 1146–56 (2022) (explaining the ownership of TikTok, congressional inquiries, and the proposed ban).

In today's data-driven world, the transfer of data from corporation to corporation, or country to country, is an essential part of international trade.[33] A business may need to transfer data for a variety of reasons, including, but not limited to, providing data to suppliers, sharing data with business partners, increasing operational efficiency, or for purposes of corporate acquisition or merger.[34]

When entities transfer data, two key stakeholders—data processors and data controllers—are used to effect the transfer.[35] A data controller "determines the purposes for which and the means by which personal data is processed."[36] Thus, an entity acts as a data controller if it decides "why" and "how" personal data should be processed.[37] An employee of the entity, acting as its agent, fulfills the entity's tasks as a data controller by "processing personal data within [the] organisation."[38] A data processor, in contrast, "is usually a third party external to the company"[39] that "processes personal data only on behalf of the controller."[40]

While data usage and storage has been vilified in the news at times,[41] it can also make everyday life better. For example, Spotify

---

33 *Data Protection Guide for Small Businesses: International Data Transfers*, EUR. DATA PROT. BD. [hereinafter *Data Protection Guide for Small Businesses*], https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en [https://perma.cc/4XY2-MYYT] (last visited Mar. 12, 2023).

34 *See Top Ten Benefits of Data Sharing in Business and Healthcare*, ATLAN (Dec. 13, 2023), https://atlan.com/benefits-of-data-sharing/ [https://perma.cc/J5J8-PBRG]; *see also Data Protection Guide for Small Businesses*, *supra* note 33.

35 *What Is a Data Controller or a Data Processor?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en [https://perma.cc/6T3G-4Q32] (last visited Apr. 3, 2024).

36 *Id.* (emphasis omitted).

37 *Id.*

38 *Id.*

39 *Id.* (emphasis omitted).

40 *Id.*

41 *See, e.g.*, Daron Acemoglu & Simon Johnson, *Big Tech Is Bad. Big A.I. Will Be Worse*, N.Y. TIMES (June 9, 2023), https://www.nytimes.com/2023/06/09/opinion/ai-big-tech-microsoft-google-duopoly.html [https://perma.cc/Z9DP-GTGP] ("History has shown us that when the distribution of information is left in the hands of a few, the result is political and economic oppression."); Scott Thomson, *The Dangers of Too Much Data*, BUILT IN (July 11, 2023), https://builtin.com/data-science/dangers-of-too-much-data [https://perma.cc/LU4J-NWEG]; Solan Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 671 (2016) (discussing how "[u]nthinking reliance on data mining can deny historically disadvantaged and vulnerable groups full participation in society"). Big data has also been used by authoritarian governments, such as China, to

recently implemented the use of Artificial Intelligence to generate "daylists," or daily playlists, for users based on their listening habits throughout the day—using and storing data about each user's musical preferences.[42] Data collection also helps healthcare systems track and maintain personal health records, predict the transmission of disease, and devise treatment protocols and potential cures.[43] Regardless of whether big data is morally "good" or "bad" for society, it is here to stay,[44] and its use will continue to become a more prominent part of everyday life.[45]

---

disadvantage citizens whom the government deems to conduct themselves in an unsavory manner (e.g., criticizing government actions on social media or online platforms). *See* Nicole Kobie, *The Complicated Truth About China's Social Credit System*, WIRED (June 7, 2019, 7:00 AM), https://www.wired.com/story/china-social-credit-system-explained/ [https://perma.cc/6AMY-JEKC]; Katie Canales & Aaron Mok, *China's 'Social Credit' System Ranks Citizens and Punishes Them with Throttled Internet Speeds and Flight Bans if the Communist Party Deems Them Untrustworthy*, BUS. INSIDER (Nov. 28, 2022, 2:52 PM), https://www.yahoo.com/news/chinas-social-credit-system-ranks-123042422.html [https://perma.cc/P7B3-6JK4]. *But see* Zeyi Yang, *China Just Announced a New Social Credit Law*, MIT TECH. REV. (Nov. 22, 2022), https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/ [https://perma.cc/F77L-HFJ5] (explaining that Western criticism of the program is somewhat misplaced, as "the system that the central government has been slowly working on is a mix of attempts to regulate the financial credit industry, enable government agencies to share data with each other, and promote state-sanctioned moral values—however vague that last goal in particular sounds").

42 *Get Fresh Music Sunup to Sundown with Daylist, Your Ever-Changing Spotify Playlist*, SPOTIFY: FOR THE RECORD (Sept. 12, 2023), https://newsroom.spotify.com/2023-09-12/ever-changing-playlist-daylist-music-for-all-day/ [https://perma.cc/6YJN-M9B9] (explaining how the "daylist" function works); Mike Kaput, *How Spotify Uses AI (and What You Can Learn from It)*, MKTG. A.I. INST. (Jan. 26, 2024), https://www.marketingaiinstitute.com/blog/spotify-artificial-intelligence [https://perma.cc/69YF-E78A] (discussing how Spotify uses AI to improve its user experience, including the "daylist" function).

43 *Eight Ways Big Data Affects Your Personal Life*, MICH. TECH. (Apr. 30, 2020), https://web.archive.org/web/20201031072303/https://onlinedegrees.mtu.edu/news/ways-big-data-affects-your-personal-life [https://perma.cc/WBG7-KJ44].

44 *'Big Data': Here to Stay.... but What Is It?*, SOC'Y FOR COMPUTS. & L. (June 17, 2014), https://www.scl.org/3114-big-data-here-to-stay-but-what-is-it/ [https://perma.cc/7MCU-7A8V]; Sheryl Warf, *IDC: Big Data Analytics Software Market to Record Strong Growth*, QUANTEXA CMTY., https://community.quantexa.com/discussion/1173/idc-big-data-analytics-software-market-to-record-strong-growth [https://perma.cc/63MH-542T] (Feb. 2023) (explaining that "[t]he trend of companies relying on data manipulation to analyze, predict, and swiftly adapt to changing market conditions is here to stay, being fueled by ongoing supply chain and demand shift challenges," and noting that "[i]n the first half of 2022, the EMEA BDA market posted year-on-year revenue growth of 10% in U.S. dollars, while growth in constant currency reached 19.5%").

45 *See* Terence Mills, *Big Data Is Changing the Way People Live Their Lives*, FORBES (May 16, 2018, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/05/16/big-data-is-changing-the-way-people-live-their-lives/?sh=1d0f41e73ce6 [https://perma.cc/VP6Q-

With big data's emergence, corporations and other entities increasingly rely on user data, making data transfers progressively more common in daily life. The use and storage of personal data has thus become necessary to the everyday operations of most corporations.

B. The Basics of Cross-Border Data Transfers

A data transfer is "the process of moving data from one location to another, either within a single device or between devices and networks."[46] Data is first divided into packets which contain a portion of the data and associated metadata.[47] These data packets are then transferred "over a network using wired connections like Ethernet or wireless connections like Wi-Fi . . . to their destination using IP addresses."[48] This is not, however, the only form in which a data transfer may occur. Data can be transferred using a USB or HDMI for direct device connections.[49]

Transferring data, while deceptively simple in theory, carries significant risk for entities seeking to move large amounts of information.[50] Cybercriminals have taken advantage of the increase in corporate use of data, finding more ways to steal data given its high value in the modern economy.[51] Data transfers do not only carry risks to the individuals or corporations whose data may be stolen by cyber thefts: "Generally, risks with data transfer can include threats to your infrastructure, users, data, services, and operations."[52] Absent proper protections during a

---

K4VX]; Jonathan Shaw, *Why "Big Data" Is a Big Deal*, HARV. MAG. (Mar.–Apr. 2014), https://www.harvardmagazine.com/2014/02/why-big-data-is-a-big-deal [https://perma.cc/698L-KVAQ].

46 Marshall Gunnell & Natalie Medleva, *Data Transfer*, TECHOPEDIA, (Aug. 14, 2024), https://www.techopedia.com/definition/18715/data-transfer [https://perma.cc/5ANF-SNCP].

47 *See id.*

48 *Id.*

49 *Id.*

50 *See* Canadian Ctr. for Cyber Sec., *Data Transfer and Upload Protection - ITSAP.40.212*, GOV'T OF CAN. (Dec. 14, 2022), https://www.cyber.gc.ca/en/guidance/data-transfer-upload-protection-itsap40212 [https://perma.cc/K5XD-HYZD].

51 *See id.*

52 *Id.* In 2023, the FBI released a cybercrimes report which found that healthcare, critical manufacturing, and government facilities were targeted with more ransomware attacks than any other critical U.S. infrastructure. *See* Tina Reed, *Health Care Was Biggest Victim of U.S. Ransomware Attacks Last Year*, AXIOS (Mar. 11, 2024), https://www.axios.com/2024/03/11/health-care-ransomware-attacks [https://perma.cc/5AMK-

data transfer, "leakage"[53] can occur, making data vulnerable to cybercriminals.[54] For example, threat actors[55] are "individuals or groups that intentionally cause harm to digital devices or systems."[56] They exploit gaps in data transfers to steal sensitive data[57] or restrict an organization's access to their system, threatening to return access only if a ransom is paid (also known as a "ransomware" attack).[58]

Statistics concerning ransomware and phishing attacks reveal the importance of protecting information, especially during times when the data is most vulnerable, primarily during data transfers. Between 2022 and 2023, "[t]he X-Force Threat Intelligence Index found that ransomware infections declined by

---

LRCP]. Furthermore, "[t]he Internet Crime Complaint Center, or IC3, received more than 2,800 complaints identified as ransomware that caused adjusted losses of nearly $60 million in 2023," which included "1,193 complaints from organizations that are part of what the FBI categorizes as belonging to 'critical' infrastructure." *Id.*

53 *See Data Leakage: Common Causes, Examples & Tips for Prevention*, BLUEVOYANT, https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention [https://perma.cc/3HW3-7V9G] (last visited Mar. 16, 2024) (explaining that "[d]ata leakage occurs when sensitive data gets unintentionally exposed to the public in transit, at rest, or in use"). Data leakage is different than a data breach; a data breach is dissimilar from leakage because a data breach is usually the result of an external intrusion (a cyberattack), while a data leak is usually caused by employee negligence (poor e-mail and data transfer practices). *See id.*

54 Data leakage can still expose vulnerabilities in data protection because it "can result in a data breach but does not require exploiting unknown vulnerabilities." *Id.* ("For example, a misconfigured Amazon Web Services (AWS) S3 bucket can cause a leak. S3 buckets provide cloud storage space for uploading files and data.").

55 Throughout this Article, "threat actors" will be used to refer to the malicious actors that conduct cybercrimes to exploit sensitive data. *See generally What Is a Threat Actor?*, IBM, https://www.ibm.com/topics/threat-actor [https://perma.cc/XY2Q-98UC] (last visited Aug. 31, 2024).

56 *Id.*

57 *See, e.g.*, *Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 29, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b [https://perma.cc/6W6C-3QKB]. For further discussion on threat actors, see *Threat Actor*, NIST, https://csrc.nist.gov/glossary/term/threat_actor [https://perma.cc/H8F4-PX7L] (last visited Aug. 31, 2024).

58 Matthew Kosinski, *What Is Ransomware?*, IBM, https://www.ibm.com/topics/ransomware [https://perma.cc/GPW9-MZE7] (June 4, 2024). Recently, "ransomware attacks have evolved," including "double-extortion and triple-extortion tactics that raise the stakes considerably." *Id.* IBM reported:

> Even victims who rigorously maintain data backups or pay the initial ransom demand are at risk. Double-extortion attacks add the threat of stealing the victim's data and leaking it online. Triple-extortion attacks add the threat of using the stolen data to attack the victim's customers or business partners.

Id.

11.5%."[59] But despite that good news, this promising trend was eclipsed by the drastic decrease in time it took threat actors to commit a ransomware attack.

The decrease is likely due to defenders becoming more successful in detecting and preventing ransomware attacks. This positive finding is tempered by the fact that the average attack timeline is just four days: "This speed gives organizations little time to detect and thwart potential attacks."[60]

With the decrease in the time it takes for a threat actor to infiltrate a system, and with the increase in attacks, organizations have less time to react to the threat.[61] Ransom demand amounts, while rarely disclosed by corporations, are reaching seven- and eight-figure amounts.[62] The spike in ransomware amounts, coupled with the decrease in time to thwart attacks, has increased the amount of risk for an entity that uses data.[63] Due to the elevated risk associated with handling data, it is more important than ever for entities to ensure proper risk mitigation during data transfers, especially concerning those that cross borders.

III. THE CURRENT STATE OF PRIVACY LAWS AFFECTING TIKTOK'S DATA STORAGE AND TRANSFER: A BRIEF OVERVIEW

Privacy and cybersecurity laws are relatively novel, with the first federal law dating back to the Computer Security Act of 1987,[64] and the earliest data breach notification law in the United States dating back to 2003.[65] Privacy law development has been characterized as a dialogue between the judicial and legislative branches about its scope and application, where "[i]n

59 *Id.* (emphasis omitted).

60 *Id.* For a discussion on current events in cybersecurity, see Mateo Formaggi, *Cybercrime and Ransomware*, 37 INT'L ENF'T L. REP. 401 (2021). For more information on ransomware, see Edward A. Morse & Ian Ramsey, *Navigating the Perils of Ransomware*, 72 BUS. L. 287 (2017) (providing an overview of ransomware, as well as discussing the risks to organizations and corporations that are the targets of such attacks).

61 *See* Kosinski, *supra* note 58.

62 *Id.*

63 *See generally id.*

64 For a comprehensive timeline of cybersecurity law advancements, see *NIST Cybersecurity Program History and Timeline*, NIST, https://csrc.nist.gov/nist-cyber-history [https://perma.cc/2UWN-ADQM] (last visited Mar. 18, 2024).

65 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 1 (2019).

some matters, courts will define new privacy rights."[66] Recently, privacy laws have emerged as a hot-button issue, especially in the context of using and selling personal data.[67] With the emergence of data usage as a critical part of most businesses, many states have passed laws preventing business entities from using consumer data without consent, imposing the requirement that they provide consumers with notice before collecting data,[68] among other consumer protection provisions.[69]

The U.S. Congress has failed to pass any sweeping privacy protections,[70] instead delegating the states to pass their own legislation. At the time of writing this Article, thirteen states have passed individual consumer privacy protection laws.[71] Overseas, the EU was one of the first major governmental bodies to enact a consumer data privacy protection law, requiring each member state to implement it by May 25, 2018.[72] Since then, approximately 71% of countries have passed privacy legislation, with 9% of countries having drafted but not passed privacy legislation, 15% of countries having no legislation concerning

66 *Id.*

67 *See, e.g.*, Brian Fung, *Feds Crack Down Hard on Selling of Personal Data Without Consent*, CNN (Jan. 19, 2024, 2:13 PM), https://www.cnn.com/2024/01/19/tech/ftc-crackdown-data-inmarket-media/index.html [https://perma.cc/M6RF-QAMT] (discussing the Federal Trade Commission's recent ban on corporations selling consumers' personal data without consent); David McCabe, *Biden Acts to Stop Sales of Sensitive Personal Data to China and Russia*, N.Y. TIMES (Feb. 28, 2024), https://www.nytimes.com/2024/02/28/technology/biden-data-sales-china-russia.html [https://perma.cc/F9VZ-3ULR] (explaining the recent presidential order by President Biden that bans the mass sale of consumer data to China and Russia); Sean Lyngaas, *Researchers Find Sensitive Personal Data of US Military Personnel Is for Sale Online*, CNN (Nov. 6, 2023, 9:43 AM), https://www.cnn.com/2023/11/06/politics/data-of-military-personnel-for-sale-online/index.html [https://perma.cc/QA5U-6FUB].

68 *See, e.g.*, CPRA, 2020 Cal. Legis. Serv. Proposition 24 (West) (codified at CAL. CIV. CODE §§ 1798.100–.199.100); COLO. REV. STAT. ANN. § 6-1-713.5 (West 2024); Colorado Privacy Act, COLO. REV. STAT. ANN. §§ 6-1-1305 to -1313 (West 2024).

69 *See, e.g.*, Washington My Health, My Data Act, WASH. REV. CODE § 19.373 (2024); Florida Digital Bill of Rights, Fla. Stat. § 501.702(9)(a)(5) (2024). For more information on the individual rights that each state law gives to consumers, see Folks, *supra* note 14.

70 *See, e.g.*, Informing Consumers About Smart Devices Act, S. 90, 118th Cong. (2023); *see also* Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, BROOKINGS (Jan. 14, 2021), https://www.brookings.edu/articles/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ [https://perma.cc/AU38-8JEC].

71 *See* Folks, *supra* note 14.

72 *See* GDPR, *supra* note 22.

privacy, and the remaining 5% of countries having provided no data on the matter.[73]

China is also among the major countries passing privacy legislation.[74] The China Personal Information Protection Law (PIPL) applies "to organizations and individuals who process personally identifiable information (PII) in China, but also those who process data of Chin[ese] citizens' PII outside of China," and requires subjects to be provided with a privacy notice, the purpose and method of collection, and other requirements.[75]

While an in-depth discussion of each state privacy law in the United States is beyond the scope of this Article, a brief overview of relevant privacy laws in China, Malaysia, and Texas will be discussed below to provide context regarding TikTok data transfers.[76]

A. Current State of Privacy Laws in China

In the early 2000s, China began "establish[ing] a legal framework for privacy and personal information protection."[77] This effort led to China's congressional body passing a series of laws,[78] including PIPL.[79] On August 20, 2021, the thirtieth

---

73 *Data Protection and Privacy Legislation Worldwide*, *supra* note 20 ("Africa and Asia show different level[s] of adoption with 61 and 57 per cent of countries having adopted such legislations. The share in the least developed countries in [sic] only 48 per cent.").

74 *See China Privacy Law*, BERKELEY OFF. OF ETHICS, https://ethics.berkeley.edu/privacy/international-privacy-laws/china-privacy-law [https://perma.cc/AVQ3-8E2D] (last visited Mar. 18, 2024) (explaining the basic principles of China's Personal Information Protection Law).

75 *Id.*

76 It is worth noting that TikTok is incorporated under ByteDance in the Cayman Islands and is based out of both California and Singapore. *See* Joe McDonald & Zen Soo, *Why Does US See Chinese-Owned TikTok as a Security Threat?*, ASSOCIATED PRESS (Mar. 24, 2023, 7:24 AM), https://apnews.com/article/tiktok-bytedance-shou-zi-chew-8d8a6a9694357040d484670b7f4833be [https://perma.cc/5KDD-8P63]. Since TikTok does not claim to store its data in California, the Cayman Islands, or Singapore, these locations' privacy laws will not be discussed and are beyond the scope of this Article.

77 Chengxin Peng, Guosong Shao & Wentong Zheng, *China's Emerging Legal Regime for Privacy and Personal Information Protection*, 15 TSINGHUA CHINA L. REV. 191, 193 (2023) (discussing the emerging legal regime to protect Chinese citizens' personal data).

78 One example is the Tort Law of 2009, which "for the first time, formally included the right to privacy as one of [the] protected civil rights." *Id.* at 193 n.3; *see also Tort Liability Law of the People's Republic of China*, THE CENT. PEOPLE'S GOV'T OF THE PEOPLE'S REPUBLIC OF CHINA (Dec. 26, 2009), https://www.gov.cn/flfg/2009-12/26/content_1497435.htm [https://perma.cc/S2V9-8RN8]. It is worth noting that China's cultural definition of privacy is very different than its western counterpart. Specifically, "privacy is not part of our traditional culture [but rather is] imported from the West into

meeting of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China (NPC) enacted PIPL.[80] PIPL went into effect on November 1, 2021, and "provides direction on many topics, including rules for the processing of personal and sensitive information . . . ."[81] PIPL "also introduces rules for personal information protection processors [and] data subject rights, [as well as] outlines requirements regarding international data transfers to third parties."[82]

Specifically concerning data transfers, "Article 38 of PIPL . . . provides several conditions (or legal paths) that must be met before a cross-border data transfer may occur."[83] To satisfy Article 38, the transfer must have either: (1) "passed the security assessment organized by the State cyberspace administration in accordance with Article 40 hereof"; (2) "been certified by a specialized [body] in accordance with the provisions of the State cyberspace administration in respect of the protection of personal information"; (3) "concluded a contract with an overseas recipient according to the standard contract formulated by the State cyberspace administration, specifying the rights and obligations of both parties"; or (4) "satisfied other conditions prescribed by laws, administrative regulations, or the State cyberspace administration."[84]

Article 38 denotes specific requirements that a data handler must satisfy to transfer Chinese citizens' data outside the

---

our system." Sam Pfeifle, *China's Evolving Views on Privacy*, IAPP (Sept. 28, 2017), https://iapp.org/news/a/chinas-evolving-views-on-privacy/ [https://perma.cc/TDD5-CQXS] (quoting a close adviser to the Chinese government). Instead, China "recognize[s] privacy as a civil right, as a right relating to the civil code," rather than a "constitutional right," and is for "the purpose of promoting social harmony, and, therefore, this is very different from the western system, which is based on human rights and freedoms." *Id.*

79 *See Rules for Cross-Border Provision of Personal Information*, PIPL PERS. INFO. PROT. L. (Mar. 2, 2022), https://personalinformationprotectionlaw.com/PIPL/category/rules-for-cross-border-provision-of-personal-information/ [https://perma.cc/TSX3-8SZU].

80 *Personal Information Protection Law of the People's Republic of China*, PIPL PERS. INFO. PROT. L., https://personalinformationprotectionlaw.com/ [https://perma.cc/U8GJ-F2QG] (last visited Mar. 18, 2024).

81 *Id.*

82 *Id.*

83 Samuel Yang, Christopher Fung & Leann Wu, *Will China's New Certification Rules Be a Popular Legal Path for Outbound Data Transfers?*, IAPP (Aug. 16, 2022), https://iapp.org/news/a/will-chinas-new-certification-rules-be-a-popular-legal-path-for-outbound-data-transfers/ [https://perma.cc/2YN3-3ZMG].

84 *Rules for Cross-Border Provision of Personal Information*, *supra* note 79.

country's border.[85] In 2022, Chinese lawmakers made it more challenging to transfer data outside of the country by permitting only the following mechanisms to conduct a data transfer: (1) "successful completion of a government-led security assessment"; (2) "obtaining certification under a government-authorized certification scheme"; or (3) "implementing a standard contract with the party(-ies) outside of China receiving the data."[86]

On June 30, 2022, China released draft provisions for public consultation which stated that "only companies that meet certain thresholds can rely on the standard contract to transfer personal information overseas."[87] Furthermore, the standard contract proposed in the draft provisions is limited to "a 'personal information processing entity' . . . which is essentially equivalent to a 'data controller' under the . . . 'GDPR.'"[88] Lastly, the contract would have to be filed with the government, with uncertainty about whether the document will be redacted in any way on a public docket.[89] Yet, this option is only available to a corporation that: (1) "is not a Critical Information Infrastructure (CII) operator"; (2) "processes the personal information of less than 1 million individuals"; (3) "has transferred the personal information of less than 100,000 individuals on a cumulative basis since January 1 of the previous year"; and (4) "has transferred the sensitive personal information of less than 10,000 individuals on a cumulative basis since January 1 of the previous year."[90]

Lastly, a corporation may file for certification with China to engage in cross-border transfers.[91] The certification "is intended to provide a basis for the implementation of one of the personal information protection certification schemes under the PIPL, namely, the certification for processing activities involving certain cross-border data transfers," and is similar in nature to

---

85 *See generally id.*

86 Yan Luo & Xuezi Dan, *Cross-Border Data Transfer Developments in China*, COVINGTON (July 2, 2022), https://www.insideprivacy.com/international/china/cross-border-data-transfer-developments-in-china/ [https://perma.cc/9MU3-BK72].

87 *Id.*

88 *Id.* (emphasis omitted).

89 *Id.*

90 *Id.*; *see also* Qian Sun, *Cross-Border Data Transfer Mechanism in China and Its Compliance*, CAL. LAWS. ASS'N (Mar. 10, 2023), https://calawyers.org/business-law/cross-border-data-transfer-mechanism-in-china-and-its-compliance/ [https://perma.cc/6RWL-V7LL].

91 Luo & Dan, *supra* note 86.

the EU's Binding Corporate Rules.[92] China's certification process is similar to the EU's Binding Corporate Rules, in that "both are intended for use by multinational companies and both set forth detailed information to be specified in a legally binding and enforceable agreement between/among the parties."[93] While the EU's Binding Corporate Rules are similar in some aspects to China's certification process, there are also notable differences:

> [T]he overseas recipient needs to promise to accept the supervision of the Chinese certification body and "accept the jurisdiction of the relevant Chinese laws and regulations on personal information protection", while in the BCR, the EU party with delegated responsibilities commits to submit to the jurisdiction of the courts, or other competent authorities in the EU, in case of violation of the BCR by a non-EU party.[94]

The stringency of these provisions led China to relax the requirements for cross-border data transfers on March 22, 2024, just six months after drafting proposed updates to PIPL.[95] Some key changes made include the distinction that "non-important" data, or data that is "collected and generated during activities such as 'international trade, cross-border transportation, academic cooperation, cross-border manufacturing or marketing' is exempted . . . if the data does *not* contain personal information or important data."[96] Additionally, a data processing entity[97] must declare important data that is to be transferred.[98] The new provisions also allow the transfer of emergency data ("transfers . . . necessary to protect the life, health, and physical

---

92 *Id.*

93 *Id.*

94 *Id.*

95 *See* Yan Luo & Xuezi Dan, *China Eases Restrictions on Cross-Border Data Flows*, COVINGTON & BURLING LLP (Mar. 25, 2024), https://www.insideprivacy.com/uncategorized/china-eases-restrictions-on-cross-border-data-flows/ [https://perma.cc/4R78-JGZ5].

96 *Id.* (emphasis added).

97 Under PIPL, a "handler" is a data controller designated by a non-Chinese corporation during a data transfer to oversee the transfer. *China's Personal Information Protection Law (PIPL)*, UC IRVINE OFF. OF RSCH. (Mar. 9, 2022), https://news.research.uci.edu/irb-hrp/chinas-personal-information-protection-law-pipl/ [https://perma.cc/978Z-86XT]. Corporations seeking to conduct a cross-border transfer of information from China to an outside country must designate a "handler" (or "controller," the term used by GDPR) to be responsible for transferring the information outside China. *Id.* This handler reports to the Chinese government. *Id.* Furthermore, transfers of "sensitive data out of Mainland China . . . must be assessed and approved by the Cyberspace Administration of China." *Id.*

98 Luo & Dan, *supra* note 95.

safety of a natural person") and employee data that is necessary to carry out "cross-border human resources management."[99] Thus, while the new provisions provide carveouts for specific types of data transfers, many of the strict requirements—such as a contract on file with the government—still exist.[100]

B. Current State of Privacy Laws in Malaysia

Malaysia passed its first comprehensive data protection law in 2010, titled the Personal Data Protection Act (PDPA).[101] Malaysia's PDPA was passed by the Malaysian Parliament on June 2, 2010, and went into force on November 15, 2013.[102] Since the initial passing of the PDPA, the Malaysian Personal Data Protection Commissioner has identified twenty-two main issues with its administration and enforcement, five of which have been targeted in proposed amendments to the PDPA.[103] These five amendments were proposed but tabled in October 2022.[104] The next year, in October 2023, Malaysia's Deputy Minister of Communications, Teo Nie Ching, announced that "preparation of the bill to amend the PDP is in the final stages" and that she expects Malaysia's legislative body to review the proposals in March 2024.[105] By the end of October 2024, the bill had received royal assent and was published in Malaysia's *Federal Gazette*, with its provisions scheduled to become effective in early 2025.[106]

---

99 *Id.*

100 *See id.* Other carveouts include an exemption "based on 'negative lists' established by free trade zones" and "data originating outside of China that merely transits through China without involving any domestic personal information or important data." *Id.* Furthermore, the newer, relaxed provisions still require notice, separate consent for the transfer, and a personal information protection impact assessment, as outlined in Article 10 of PIPL. *Id.*

101 Personal Data Protection Act 2010 (Act 709) (Malay.).

102 DLA PIPER, DATA PROTECTION LAWS OF THE WORLD: MALAYSIA 2 (2023), https://www.dlapiperdataprotection.com/?t=law&c=MY [https://perma.cc/MJ79-GNTT] (click "DOWNLOAD current countries" hyperlink).

103 *Id.*

104 *Id.*; *see also Cloud Compliance Center: Malaysia*, BAKER MCKENZIE, https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/apac/malaysia/ [https://perma.cc/FQ99-3T7M] (last visited Apr. 11, 2024).

105 DLA PIPER, *supra* note 104, at 2.

106 *News Alert: The Gazetting of the Personal Data Protection (Amendment) Act 2024*, RAJAH & TANN ASIA (Oct. 22, 2024), https://www.rajahtannasia.com/viewpoints/news-alert-the-gazetting-of-the-personal-data-protection-amendment-act-2024/ [https://perma.cc/7HXU-3NYJ]; Robert Healey, *Navigating Malaysia's Personal Data Protection Amendment Bill 2024: Are You Ready for PDPA Compliance?*, FORMITI, https://formiti.com/navigating-

In its pre-amendment state, the law was widely regarded as inadequate at addressing data privacy issues, especially in contrast with the more recently updated and robust GDPR.[107] The Malaysian PDPA is a reactive law, designed mainly to create criminal liability for violations of the law:

> The [PDPA] primarily focuses on regulating criminal and constitutional aspects of privacy breaches. Laws, such as the Personal Data Protection Act 2010 (Malaysia) and the Penal Code (Malaysia), only provide criminal sanctions in cases where an individual's privacy is violated. The protection of personal liberties, including the right to privacy, is outlined in Article 5(1) of the Federal Constitution (Malaysia). However, constitutional protection *only offers remedies for privacy breaches committed by the executive and legislative branches of the government*, excluding infringements of privacy between private individuals. As a result, there is a clear gap or deficiency in Malaysian law . . . .[108]

In a cybersecurity breach in 2022, Malaysia's PDPA was put to the test and largely failed.[109] Malaysia experienced a major governmental cybersecurity breach when "personal details of 22 million Malaysians, allegedly from the National Registration Department, were leaked and sold online."[110] While the Malaysian government subsequently launched an investigation, the government largely downplayed what had occurred.[111] No fines were ever issued.[112] Although this is only one incident, it reveals much about the inadequacy of the current data security and privacy laws in Malaysia, especially as compared to GDPR.

---

malaysias-personal-data-protection-amendment-bill-2024-are-you-ready-for-pdpa-compliance/ [https://perma.cc/F7C4-EHZU] (last visited Dec. 21, 2024).

107 Adnan Trakic et al., *It Is Time to Recognize the Tort of Invasion of Privacy in Malaysia*, 13 INT'L DATA PRIVACY L. 229, 310 (2023) ("In contrast to European countries, the status of privacy laws in Malaysia is regarded as inadequate. There is a notable absence of comprehensive legal frameworks for privacy protection, with the Personal Data Protection Act 2010 (the 'PDPA') being the primary legislation that addresses only data protection concerns."); *see also* Aaron Raj, *Is Data Privacy Just a Pipedream in Malaysia?*, TECHWIRE ASIA (Feb. 2, 2023), https://techwireasia.com/02/2023/is-data-privacy-just-a-pipe-dream-in-malaysia/ [https://perma.cc/3FQN-JJ6D] (explaining that Malaysia has fallen short on enforcement of its data protection laws).

108 Trakic et al., *supra* note 107, at 300 (emphasis added).

109 Raj, *supra* note 107.

110 *Id.*

111 *Id.*; *see also Data of 22.5 Million Malaysians Born 1940-2004 Allegedly Being Sold for US$10k*, STRAITS TIMES (May 18, 2022, 5:52 PM), https://www.straitstimes.com/asia/se-asia/data-of-225-million-malaysians-born-1940-2004-allegedly-being-sold-for-us10k [https://perma.cc/3RVM-ZMBT].

112 Raj, *supra* note 107.

Concerning cross-border transfers, Malaysia currently prohibits the transfer of Malaysian users' data outside the country "unless the Malaysian Minister of Communications and Digital has specifically exempted the jurisdiction from the restriction via publication" in the *Federal Gazette*, a mechanism for issuing official government notices.[113] As of April 2024, "the Minister has yet to specify any country to which personal data may be transferred without any restrictions."[114]

C. Current State of Privacy Laws in Texas

In the United States, TikTok primarily stores data in Virginia and Oregon.[115] However, it anticipates moving all of its U.S. users' data from these physical storage locations to Oracle cloud servers; this endeavor has been named "Project Texas."[116] Oracle Corporation is a company based in Austin, Texas, and is subject to the privacy laws of the state.[117]

On June 18, 2023, Texas became the tenth state to enact comprehensive data privacy legislation.[118] The Texas Data and Privacy Security Act (TDPSA) is effective as of July 1, 2024, and shares many salient features with other states' privacy laws, such as those of Utah, Colorado, and Connecticut.[119] The TDPSA

---

113 *Cloud Compliance Center: Malaysia*, *supra* note 104.

114 *Id.*

115 Mary Zhang, *TikTok's Data Center Locations and Use of Oracle Cloud*, DGTL INFRA (Feb. 18, 2024) https://dgtlinfra.com/tiktok-data-centers-cloud-locations/ [https://perma.cc/ALQ4-2QLX].

116 *Id.*; *When Will Project Texas Be Fully Operational?*, TIKTOK: U.S. DATA SEC., https://usds.tiktok.com/when-will-project-texas-be-fully-operational/ [https://perma.cc/BE24-LPKV] (last visited Dec. 21, 2024) (describing Project Texas as an ongoing effort).

117 *See id.*; Emily Baker-White, *Leaked Audio from 80 Internal TikTok Meetings Shows that US User Data Has Been Repeatedly Accessed from China*, BUZZFEED NEWS (June 17, 2022, 9:31 AM), https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access [https://perma.cc/R77Y-2U3B] ("TikTok would hold US users' protected private information, like phone numbers and birthdays, exclusively at a data center managed by Oracle in Texas (hence the project name).").

118 F. Paul Pittman & Abdul M. Hafiz, *Texas Passes Comprehensive Data Privacy Law*, WHITE & CASE LLP (July 19, 2023), https://www.whitecase.com/insight-alert/texas-passes-comprehensive-data-privacy-law [https://perma.cc/RJ8N-Z4X4]; TEX. BUS & COM. CODE ANN. §§ 541.001–.205 (West 2024); Joe Duball, *Texas Latest to Add Comprehensive State Privacy Law*, IAPP (June 2, 2023), https://iapp.org/news/a/texas-latest-to-add-comprehensive-state-privacy-law/ [https://perma.cc/96FP-C8EN].

119 Pittman & Hafiz, *supra* note 118. It is worth noting that the "majority of the law takes force 1 July 2024 while provisions for recognition of universal opt-out mechanisms take effect 1 Jan. 2025." *Texas' Comprehensive Privacy Bill Signed into Law*, IAPP (June 20, 2023), https://iapp.org/news/b/texas-comprehensive-privacy-bill-signed-into-law

confers data rights upon individuals, including the right to access, delete, correct, and opt out of sales.[120] It applies to any corporation that "conducts business in Texas or produces products or services that are consumed by Texas residents (which is likely broader than the 'targeting' language seen in certain other State Data Privacy Laws)."[121] Similar to most other state privacy laws, Texas does not provide a private right of action for privacy violations.[122] Additionally, similar to the GDPR and some other states, Texas defines differences between processors and controllers, and delegates responsibilities of each.[123] Data controllers are obligated, inter alia, to: (1) "[l]imit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to disclosed purposes for which such data is processed"; (2) "[a]dopt and implement reasonable administrative, technical, and physical data security practices"; (3) "[c]learly disclose if the controller sells consumers' sensitive personal data or biometric data"; and (4) "[w]hen in possession of de-identified data, take reasonable measures to ensure that the data cannot be associated with an individual, commit publicly to maintaining data as de-identified data, and obligate any recipients of the data to comply with the TDPSA."[124]

While the law is considered comprehensive, and does define a "[s]ale of personal data" as "the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to the third party," it does not define cross-border data transfers between states or countries.[125]

[https://perma.cc/CCZ4-98CH]; *see also* Matt Stringer, *New Texas Data and Privacy Security Act Aims to Increase Protections for Online User Data*, THE TEXAN (June 19, 2023), https://thetexan.news/state/legislature/88th-session/new-texas-data-and-privacy-security-act-aims-to-increase-protections-for-online-user-data/ [https://perma.cc/KEN2-KA3D].

120 IIAP, US STATE PRIVACY LEGISLATION TRACKER 2024, at 1 (2024), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/KAQ9-ZR2Z].

121 Devika Kornbacher, *The Texas Data Privacy Law: An Overview*, CLIFFORD CHANCE (Dec. 31, 2023), https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2023/12/the-texas-data-privacy-law-an-overview.html [https://perma.cc/29RR-EX4U] (outlining the major key takeaways from TDPSA).

122 IIAP, *supra* note 120, at 1.

123 Kornbacher, *supra* note 121.

124 Pittman & Hafiz, *supra* note 118; *see also* Natasha G. Kohne & Joseph Hold, *Texas Data Privacy Act: What Businesses Need to Know*, AKIN GUMP (July 28, 2023), https://www.akingump.com/en/insights/alerts/texas-data-privacy-act-what-businesses-need-to-know [https://perma.cc/7BMP-CUEC].

125 TEX. BUS. & COM. CODE ANN. § 541.001(28) (West 2024).

Currently, the law more clearly defines what is *not* a sale or transfer of data than what *is* the sale or transfer of data.[126] Notably absent is any policy for transferring data outside the state or country, or otherwise providing guidance beyond the handling of deidentified data, leaving corporations with little guidance for transferring consumer data through interstate commerce or abroad.

D. Current State of Privacy Laws in Singapore

Singapore governs the use and transfer of private information through its data protection law, the Personal Data Protection Act.[127] The Singaporean PDPA was enacted in 2012 and amended in 2020 to better align with GDPR.[128] The PDPA amendments took effect on February 1, 2021, and "strengthen[ed] organisational accountability and consumer protection, while giving organisations the confidence to harness personal data for innovation."[129]

The objectives of Singapore's PDPA include recognizing individual data rights, and the "need to protect individuals' personal data . . . of organisations to collect, use or disclose personal data for legitimate and reasonable purposes."[130] The PDPA is also meant to be a "data protection regime" which "safeguard[s] personal data from misuse and . . . maintain[s] individuals' trust in organisations that manage their data."[131] Finally, PDPA seeks to establish trust in entities that collect data in order to strengthen Singapore's place in the world economy.[132]

126 *See id.*

127 *PDPA Overview*, PERS. DATA PROT. COMM'N SING., https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act [https://perma.cc/UBT6-KWJQ] (last visited Apr. 11, 2024).

128 *Id.*; DLA PIPER, DATA PROTECTION LAWS OF THE WORLD: SINGAPORE 2 (2023), https://www.dlapiperdataprotection.com/?t=law&c=SG [https://perma.cc/6Y7S-NJTY].

129 *Amendments to the Personal Data Protection Act (PDPA) Take Effect from 1 February 2021*, PERS. DATA PROT. COMM'N SING. (Jan. 29, 2021), https://www.pdpc.gov.sg/news-and-events/announcements/2021/01/amendments-to-the-personal-data-protection-act-take-effect-from-1-february-2021 [https://perma.cc/46DX-YXFL].

130 *PDPA Overview*, *supra* note 127.

131 *Id.*

132 *Id.*

Furthermore, Singapore has clear policies in place that guide cross-border data transfers.[133] In 2018, Singapore was the sixth member country to join the Asia-Pacific Economic Corporation (APEC).[134] As of April 2024, Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States follow these data transfer guidelines for extraterritorial transfers.[135] APEC's cross-border transfer principles, or Cross-Border Privacy Rules (CBPRs) designated under the Cross-Border Privacy Enforcement Agreement (CPEA),[136] are designed to streamline transfer while recognizing that "regulatory barriers threaten to undermine opportunities created by the digital economy at a time when companies are relying increasingly on digital technologies and innovations to continue business operations and recover economically."[137] The CBPR system was developed with recognition "that growing Internet connectivity and the digitisation of the global economy have resulted in the rapid increase in the collection, use, and transfer of data across borders, a trend that continues to accelerate."[138] APEC's mission statement also illustrates its purpose to "bridge different regulatory approaches to data protection and privacy."[139] Similar to the EU's *Schrems II* guidance, APEC's purposes are to ensure a clear standard for data transfers, facilitate data sharing and communications

---

133 *See Singapore Joins APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems*, PERS. DATA PROT. COMM'N SING. (Mar. 6, 2018), https://www.pdpc.gov.sg/news-and-events/announcements/2018/03/singapore-joins-apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems [https://perma.cc/K5RJ-PXLU].

134 *Id.*; *see also Global Cross-Border Privacy Rules Declaration*, U.S. DEP'T OF COM., https://www.commerce.gov/global-cross-border-privacy-rules-declaration [https://perma.cc/8J7T-54UT] (last visited Apr. 11, 2024).

135 *Global Cross-Border Privacy Rules Declaration*, *supra* note 134.

136 *See APEC Cross-Border Privacy Enforcement Arrangement (CPEA)*, ASIA-PAC. ECON. COOP. [hereinafter *APEC CPEA*], https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group/cross-border-privacy-enforcement-arrangement [https://perma.cc/9X9A-Q6CY] (Feb. 2024) (outlining the principles and aims of the CPEA).

137 *Id.*

138 *Id.; see also APEC CPEA*, *supra* note 136 (outlining the principles and aims of the CPEA).

139 *Global Cross-Border Privacy Rules Declaration*, *supra* note 134. Differences between the EU's data transfer processes and APEC's processes will subsequently be discussed in comparison to the *Schrems II* decision. *See infra* Section III.B.

between countries, and address privacy challenges accompanying the use and transfer of personal data.[140]

E. Potential U.S. Federal Privacy Law

On April 7, 2024, Republican House Representative Cathy McMorris Rodgers and Democratic Senator Maria Cantwell, both serving the state of Washington, released a draft of the bipartisan American Privacy Rights Act of 2024 (Act),[141] which was introduced in the House of Representatives on June 25, 2024.[142] The surprising unveiling garnered mixed reviews and skepticism, especially from regulators in states with already robust privacy laws like California.[143] The skepticism from stakeholders is not misplaced; Congress has previously tried to pass federal privacy legislation and failed.[144]

The new 140-page Act seeks to create protections for consumers and clarify guidelines for entities to follow when

---

140 *APEC CPEA*, *supra* note 136.

141 American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. (2024).

142 *See* Jedidiah Bracy, *New Draft Bipartisan US Federal Privacy Bill Unveiled*, IAPP (Apr. 7, 2024), https://iapp.org/news/a/new-draft-bipartisan-us-federal-privacy-bill-unveiled/ [https://perma.cc/A42W-5VFX] (explaining the details and major takeaways of the proposed bipartisan bill). *See generally* Robinson & Cole LLP, *Congress Introduces Promising Bipartisan Privacy Bill*, THE NAT'L L. REV. (Apr. 11, 2024), https://natlawreview.com/article/congress-introduces-promising-bipartisan-privacy-bill [https://perma.cc/V6RF-58KL] (suggesting that, although previous attempts at passing a federal privacy law failed, this attempt seems more promising given the significant increase and usage of personal data); Bracy, *supra* note 13 (chronicling the reactions from corporations in the technology realm that believe the bill will curtail Californians' privacy rights and will create confusing opt-in/opt-out rules).

143 *See* Bracy, *supra* note 13. California Privacy Protection Agency (CPPA) Executive Director Ashkan Soltani stated that his organization is reviewing the legislation but is "disappointed that the proposed approach to preemption is substantively the same as . . . the [one the] CPPA Board voted to oppose" in the American Data Protection and Privacy Act. *Id.* Further, "Americans shouldn't have to settle for a federal privacy law that limits states' ability to advance strong protection in response to rapid changes in technology and emerging threats in policy—particularly when Californians' fundamental rights are at stake." *Id.* Soltani believes that Congress's bill is flawed and should change its approach: "Congress should set a floor, not a ceiling." *Id.*

144 *See* Müge Fazlioglu, *U.S. Federal Privacy Regulation Tracker*, IAPP, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/ [https://perma.cc/5ZRG-735B] (Aug. 2024); Jeewon K. Serrato, Shruti Bhutani Arora & Christine Mastromonaco, *The United States Moves Towards a Comprehensive Privacy Law (One More Time)*, PILLSBURY (April 22, 2024), https://www.pillsburylaw.com/en/news-and-insights/american-privacy-rights-act.html [https://perma.cc/MKK6-JATP].

handling personal information.[145] Notable provisions include an anti-discrimination clause prohibiting entities from discriminating against users based on the data collected (which appears in some form in every state privacy law passed thus far).[146] It is not clear whether the passing of this proposed Act, however, would change the U.S.-UK or EU-U.S. data bridges, but passing a sweeping law would likely improve relationships since a previous concern with data transfers from Western European nations surrounded the lack of federal privacy legislation.[147] As of April 2024, the standard for privacy transfers between the United States and EU is the EU-U.S. Privacy Shield Framework.[148]

IV. *SCHREMS* AND CPEA: CURRENT U.S. CROSS-BORDER DATA TRANSFER POLICIES

Two prevailing methods of cross-border transfers include the EU's *Schrems I* and *Schrems II* decisions,[149] the EU-U.S. Privacy Shield Framework,[150] and APEC's CPEA.[151] Each are discussed in turn below.

---

145 *See* Jennifer Gregory, *New Proposed Federal Data Privacy Law Suggests Big Changes*, SECURITYINTELLIGENCE (Mar. 1, 2024), https://securityintelligence.com/news/american-privacy-rights-act-federal-data-privacy-law/ [https://perma.cc/7HFU-X8VE]. *See generally* Cobun Zweifel-Keegan, *Top Takeaways from the Draft American Privacy Rights Act*, IAPP (Apr. 11, 2024), https://iapp.org/news/a/top-takeaways-from-the-draft-american-privacy-rights-act/ [https://perma.cc/67QJ-YFZR] (discussing key takeaways from the proposed Act, including similarities between Senator Cantwell's previous privacy bill, the Consumer Online Privacy Act, and the previously proposed American Data Privacy and Protection Act).

146 *See* Bracy, *supra* note 142.

147 *See* Kelvin Chan, *Europe Signs Off on a New Privacy Pact that Allows People's Data to Keep Flowing to US*, ASSOCIATED PRESS (July 10, 2023, 9:07 AM), https://apnews.com/article/data-privacy-cybersecurity-europe-us-7bfc7c2be54a81068b5b16dff32ed9c6 [https://perma.cc/6UPA-MYJ5] ("Washington and Brussels long have clashed over differences between the EU's stringent data privacy rules and the comparatively lax regime in the U.S., which lacks a federal privacy law.").

148 *See, e.g.*, *EU-U.S. Privacy Shield*, U.S. DEP'T OF COM., https://www.commerce.gov/tags/eu-us-privacy-shield [https://perma.cc/N5AW-EL6P] (last visited Apr. 12, 2024); *Welcome to the Data Privacy Framework (DPF) Program*, DATA PRIV. FRAMEWORK PROGRAM [hereinafter *Privacy Shield Framework*], https://www.dataprivacyframework.gov/ [https://perma.cc/TKW5-C7WR] (last visited Apr. 12, 2024); *see* discussion *infra* Section III.C.

149 Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015); Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020).

150 *Privacy Shield Framework*, *supra* note 148.

151 *APEC CPEA*, *supra* note 136.

A. *Schrems* Decisions and U.S.-EU Privacy Shield

The debate over U.S. and EU privacy policies is not a new concept; in fact, the debate over privacy governance dates back to the dawn of the internet.[152] In October 1998, the EU's Directive on Data Protection was implemented, blocking EU citizens' personal information from being transferred to countries deemed to "lack adequate protection of privacy."[153] Even then, the EU criticized America's lack of uniform privacy protections.[154] While much has changed in the data privacy and cybersecurity sector since 1998,[155] one thing has not: a lack of federal privacy laws in the United States. Comparatively, the EU has long recognized privacy as a right, beginning in 1948 with the passage of the United Nations Declaration of Human Rights.[156] In 1995, the EU passed the Data Protection Directive, which was bolstered by the Right to Be Forgotten in 2012 and supplanted by the GDPR in 2018.[157] Meanwhile, in the United States, federal legislators took a piecemeal approach, passing area-specific laws like the Privacy Act of 1974,[158] the Children's Online Privacy Protection Act,[159]

---

152 While "node-to-node" communication was first created in the late 1960s, the "birth" of the internet is said to be January 1, 1983. Evan Andrews, *Who Invented the Internet?*, HISTORY (Oct. 28, 2019), https://www.history.com/news/who-invented-the-internet [https://perma.cc/Q6XX-AS8S] (detailing events leading up to the creation of the internet and subsequent developments in internet technology post-creation).

153 Peter P. Swire & Robert E. Litan, *Avoiding a Showdown over EU Privacy Laws*, BROOKINGS INST. (Feb. 1, 1998), https://www.brookings.edu/articles/avoiding-a-showdown-over-eu-privacy-laws/ [https://perma.cc/Z4DZ-5YY4].

154 *See id.*

155 *See, e.g.*, *The 21st-Century Evolution of Cyber Security*, ICAEW (Oct. 9, 2023), https://www.icaew.com/insights/viewpoints-on-the-news/2023/oct-2023/the-21stcentury-evolution-of-cyber-security [https://perma.cc/C2PA-A563] (explaining the major evolutions in cybersecurity since the early 2000s); *History of Privacy Timeline*, UNIV. OF MICH. INFO. & TECH. SERVS.: SAFE COMPUTING, https://safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline [https://perma.cc/7W8X-4VQU] (last visited Apr. 12, 2024) (chronologizing the history of privacy rights in the United States and other major Western privacy developments, such as passing the EU Data Protection Derivative in 1995).

156 *See History of Privacy Timeline*, *supra* note 155.

157 *See id. See generally* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 (EU).

158 Privacy Act of 1974, 5 U.S.C. § 552(a).

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to 12 exceptions].

Id.

the Gramm Leach Bliley Act,[160] and the Health Insurance Portability and Accountability Act.[161]

In 2011, as a result of data transfers between the United States and EU, an Austrian student named Max Schrems filed a series of lawsuits before the Court of Justice of the European Union (CJEU).[162] "When a professor invited Facebook privacy lawyer Ed Palmieri to speak to the class, Schrems was shocked by the lawyer's limited grasp of the severity of data protection laws in Europe" and, as a result, "decided his thesis paper for the class would be about Facebook's misunderstanding of privacy law in his home continent."[163] "In the course of his research, [Schrems] discovered that Facebook's dossiers on individual users are hundreds of pages long and include information users thought had been deleted."[164] After returning to Austria, he started an activist group (on Facebook, ironically), disseminating the information he discovered.[165] The information Schrems posted garnered intense media attention, eventually leading to a probe by European privacy regulators.[166] A series of lawsuits would eventually upend the data transfer system between the two countries and create tensions between the two global forces.[167]

In *Schrems I*, *Schrems v. Data Protection Commissioner*, the CJEU invalidated the data sharing provision known as the "Safe Harbor Framework."[168] In the decision, the CJEU held that the Safe Harbor provision failed to adequately protect EU data

159 Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.

160 Gramm Leach Bliley Act, 15 U.S.C §§ 6801–6809.

161 42 U.S.C. § 1320(d); *see also Health Information Privacy Act*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/index.html [https://perma.cc/3ERR-3249] (last visited Apr. 12, 2024).

162 Ryan Beckstrom & Kyle Peterson, *US Intelligence Law & EU Data Transfer Requirements: Tools for Assessing US Law & Implementing Supplementary Measures to Meet EU Protection Levels*, 36 UTAH BAR J. 44, 44 (2023).

163 *Id.*; *see also* Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, FORBES, https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/?sh=7d0dde0d7b0b [https://perma.cc/QYU6-TLN2] (Mar. 27, 2012, 11:07 AM).

164 Hill, *supra* note 163.

165 *Id.*

166 *Id.*

167 *See id.*

168 *Schrems I*, *supra* note 149, at ¶¶ 96–106.

subjects' personal data from large-scale collection by U.S. national security and law enforcement agencies.[169]

Since 2016, the EU-U.S. Privacy Shield governed cross-border data transfers between Europe and the United States to protect European citizens' data.[170] When *Schrems II* eventually made its way to the CJEU, the result upended data transfer practices by invalidating the EU-U.S. Privacy Shield.[171] The *Schrems II* court in *Data Protection Commissioner v. Facebook Ireland Ltd.* found that U.S. surveillance laws did not afford European data subjects "adequate levels of protection as required under the [EU's] Charter of Fundamental Rights" and the GDPR.[172] Moreover, the CJEU concluded that the U.S. Foreign Intelligence Surveillance Act (FISA) infringed on EU data subjects' rights because the Act was overly broad and lacked redress.[173] Since the CJEU did not fully analyze the problematic language in FISA, some uncertainty still looms after the decision.[174]

The result of these judicial decisions, in combination with the EU's data transfer directives, created strict requirements for data transfers, leaving the United States to scramble to change its practices and policies for U.S.-EU data transfers. The CJEU's decision "maintained its position that supervisory authorities are

---

169 Robert Stankey, *EU Court Opinion Puts Pressure on Reform of U.S.-EU Safe Harbor for Data Transfers*, DAVIS WRIGHT TREMAINE LLP (Sept. 23, 2015), https://www.dwt.com/insights/2015/09/eu-court-opinion-puts-pressure-on-reform-of-useu-s [https://perma.cc/8WED-T6VH].

170 Council Regulation 2016/679, art. 45, 2016 O.J. (L 119) 1, 61(EU); *EU-U.S. Privacy Shield Framework Principles*, U.S. DEP'T OF COM., https://www.privacyshield.gov/privacy-shield-principles-full-text [https://perma.cc/3WU2-5U5T] (last visited Sept. 7, 2024). *See generally* The Harv. L. Rev. Ass'n, *National Security Law – Surveillance – Court of Justice of the European Union Invalidates the EU-U.S. Privacy Shield. – Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020)*, 134 HARV. L. REV. 1567, 1567 (2021); Press Release, U.S. Dep't of Com., U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://useu.usmission.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/ [https://perma.cc/7M2L-AWB6].

171 Council Regulation 2016/679, art. 45, 2016 O.J. (L 119) 1, 61 (EU); *EU-U.S. Privacy Shield Framework Principles*, *supra* note 170.

172 *Schrems II*, *supra* note 149, at ¶¶ 178, 185–186, 201; Council Regulation 2016/679, art. 45, 2016 O.J. (L 119) 1, 61 (EU); *see EU-U.S. Privacy Shield Framework Principles*, *supra* note 170 (explaining that under GDPR, EU data subjects have a "fundamental right" to protection concerning the processing of personal data).

173 *See Schrems II*, *supra* note 149, at ¶¶ 184, 192.

174 *See* The Harv. L. Rev. Ass'n, *supra* note 170, at 1567–68.

required to suspend or prohibit the transfer of data to the third country when it believes that the protection required by EU law cannot be ensured by other means."[175] The threat of suspending all U.S.-EU data transfers meant that entities' activities involving EU consumers could be halted indefinitely if the United States failed to address the CJEU's concerns. As a result, when entities engage in cross-border transfers between the United States and EU, the proper level of protection turns on two requirements: (1) whether "both the contractual clauses agreed between the controller or processor established in the [EU] and the recipient of the transfer established in the third country concerned"; and (2) whether, with regard to "any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country."[176] After *Schrems II*, the European Commission released Standard Contractual Clauses that must be used between controllers and processors when transferring between the two economies.[177] These clauses were meant to resolve the issue of proportionality in *Schrems II*—that legislation must include "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards."[178]

Finally, on June 18, 2021, the European Commission adopted its final Supplementary Measures Recommendations for implementation, creating a six-step roadmap to assess third-country measures to mitigate the risks that inhere when transferring data.[179] However, the European Commission's standard is still vague. Governed by the "rule of law" and "respect for human rights,"[180] the Commission's standards leave much to be desired. Although the European standard lacks

---

175 *The Definitive Guide to Schrems II*, ONETRUST DATAGUIDANCE (Nov. 22, 2022), https://www.dataguidance.com/resource/definitive-guide-schrems-ii [https://perma.cc/3R94-WCR8].

176 *Schrems II*, *supra* note 149, ¶¶ 104–105 (noting that "the assessment of the level of protection afforded in the context of such a transfer must," inter alia, consider the applicable laws of a third country "as regards any access by the public authorities of that third country to the personal data transferred," or in other words, holding that GDPR applies to data subjects' information when transferred *outside* the EU).

177 *See The Definitive Guide to Schrems II*, *supra* note 175.

178 *Schrems II*, *supra* note 149, ¶ 176; *see also* The Harv. L. Rev. Ass'n, *supra* note 170, at 1570.

179 *See The Definitive Guide to Schrems II*, *supra* note 175.

180 Council Regulation 2016/679, art. 45, 2016 O.J. (L 119) 2 (EU).

complete clarity, generally speaking, it provides more guidance than APEC's CPEA.

B. APEC's CPEA

As early as 1998, APEC published a *Blueprint for Action on Electronic Commerce*, "emphasiz[ing] that the potential of electronic commerce cannot be realised without government and business cooperation."[181] Subsequently, in 2004, APEC released a privacy framework to encourage effective privacy protection while simultaneously promoting the free flow of information and the resulting economic growth between member countries.[182] In 2007, this framework was updated and expanded on through the Data Privacy Pathfinder program, which was "aimed at promoting consumer trust and business confidence in cross-border data flows" and included "general commitments regarding the development of a Cross-Border Privacy Rules system."[183] The CPEA became effective on July 16, 2010, and was last updated in 2019.[184]

The CBPRs that govern CPEA have four main components: (1) "[r]ecognition criteria for organisations wishing to become an APEC CBPR System certified Accountability Agent"; (2) "[i]ntake questionnaire for organisations that wish to be certified as APEC CBPR System compliant by a third-party CBPR system certified Accountability Agent"; (3) "[a]ssessment criteria for use by APEC CBPR System certified Accountability Agents when reviewing an organisation's answers to the intake questionnaire"; and (4) "[a] regulatory cooperative arrangement (the CPEA) to ensure that each of the APEC CBPR system program requirements can be enforced by participating APEC economies."[185] The system is run by the Joint Oversight Panel, which administers the cross-border data transfers and ensures compliance with the CPEA.[186]

While the CPEA is meant to reduce barriers to information flow, it requires APEC member economies to "develop their own

181 *APEC CPEA*, *supra* note 136.

182 *Id.*

183 *Id.*

184 *Id.*

185 *About CBPRs*, CROSS BORDER PRIV. RULES SYS., https://cbprs.org/about-cbprs/ [https://perma.cc/9LHF-YZVH] (last visited Aug. 30, 2024); *see also Global Cross-Border Privacy Rules Declaration*, *supra* note 134.

186 *About CBPRs*, *supra* note 185.

internal business rules on cross-border privacy procedures, which must be assessed as compliant with the minimum requirements of the APEC system by . . . an Accountability Agent."[187] This system is known as an "accountability system," meaning that "when personal information is to be transferred . . . the personal information controller *should* obtain the consent of the individual *or* exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with [APEC] Principles."[188] While both have flaws, APEC's competing data transfer regime allows for more flexibility in comparison to the EU's *Schrems I* and *Schrems II* guidelines. The self-regulatory nature of APEC's data transfer rules,[189] however, could arguably leave less-responsible corporations, governed by more-relaxed enforcement agents, to handle data in such a way that exposes personal information to undue risk. In cases such as TikTok, where data subjects span the globe, the transfer and use of subject data can become complex to ensure compliance, especially when de- and re-identifying data are involved. Coupled with a lack of clear guidance from prevailing authorities, businesses like TikTok are left to their own devices to decipher these different standards. If deciphered incorrectly, incur the wrath of governments and the public alike.[190]

C. TikTok's Data Structure: Data Storage, Transfer, and Usage Practices

Beginning in early 2023, Congress has called social media magnates, including Facebook CEO Mark Zuckerberg and TikTok CEO Shou Zi Chew, to testify before Congress about their

---

187 Applications to Serve as Accountability Agents in the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System, 77 Fed. Reg. 44582 (July 30, 2012).

188 Dan Jerker B. Svantesson, *The Regulation of Cross-Border Data Flows*, 1 INT'L DATA PRIV. L. 180, 183 (2011) (emphasis added).

189 *See* W. Gregory Voss et al., *Privacy, E-Commerce, and Data Security*, 47 INT'L LAWYER 99, 110 (2013).

190 When the U.S. government compelled the CEOs of TikTok and other social media corporations to testify about their business practices and, in the case of TikTok's CEO, ties to other governments, TikTok users generally saw Congress as the problem; the hearings did not bolster public trust in social media companies either. *See* Kyle Chayka, *The TikTok Hearings Inspired Little Faith in Social Media or in Congress*, NEW YORKER (Mar. 24, 2023), https://www.newyorker.com/culture/infinite-scroll/the-tiktok-hearings-inspired-little-faith-in-social-media-or-in-congress [https://perma.cc/NE4B-2SCG].

data-use practices and marketing techniques.[191] While the main focuses of the hearings were Chew's national origin and algorithmic marketing toward children, the biggest takeaway was that Congress does not understand data privacy.[192] Although attention was directed at Chew's alleged ties to China,[193] the real issue became exceedingly clear: who has control of the data?

Per TikTok's website, the corporation stores its data in three locations: Malaysia, Singapore, and the United States.[194] For U.S. users, TikTok explains that the corporation has spent $1.5 billion on creating an ultra-secure platform that disallows "unauthorized foreign access to [user] data and the systems that deliver [that] content."[195] This system is powered by Oracle's cloud-based security structure.[196] TikTok further notes that its data security plan includes appointing other independent third-party assessors to continually check and maintain the data environment on an ongoing basis.[197] By default, TikTok stores

---

191 *Id.*; *see also Watch: Meta, TikTok and Other Social Media CEOs Testify in Senate Hearing on Child Exploitation*, PBS NEWS (Jan. 31, 2024), https://www.pbs.org/newshour/politics/watch-live-ceos-of-meta-tiktok-x-and-other-social-media-companies-testify-in-senate-hearing [https://perma.cc/W8EA-SF9Q] (summarizing the hearings where Zuckerberg and Chew were both questioned about their marketing techniques concerning their targeted practices towards children, as well as extraterritorial influence in the case of TikTok).

192 *See* Barbara Ortutay & Haleluyah Hadero, *Meta, TikTok and Other Social Media CEOs Testify in Heated Senate Hearing on Child Exploitation*, ASSOCIATED PRESS, https://apnews.com/article/meta-tiktok-snap-discord-zuckerberg-testify-senate-00754a6bea92aaad62585ed55f219932 [https://perma.cc/SL4K-H7V6] (Jan. 31, 2024, 5:26 PM) ("Sexual predators. Addictive features. Suicide and eating disorders. Unrealistic beauty standards. Bullying. These are just some of the issues young people are dealing with on social media — and children's advocates and lawmakers say companies are not doing enough to protect them."). The January 2024 hearing was not the first time Congress has questioned social media executives. *See, e.g.*, *Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation: Hearing Before the Subcomm. on Commc'ns & Tech., Subcomm. on Consumer Prot. & Com., H. Comm. on Energy & Com.*, 117th Congress 2 (2021); Chayka, *supra* note 190 (criticizing Congress and commenting that public perception of Congress's understanding of social media and technology is severely lacking).

193 *See* CNA, *"No, I'm Singaporean": TikTok CEO Chew Shou Zi Responds to U.S. Senator's Questions About China Ties*, YOUTUBE, at 0:37 (Jan. 31, 2024), https://www.youtube.com/watch?v=RgLQCfypDLk [https://perma.cc/P55F-QVD9].

194 *Who Owns TikTok?*, *supra* note 26; *see also The Truth About TikTok*, *supra* note 27.

195 *TikTok U.S. Data Security*, TIKTOK, at 0:25–0:34, https://usds.tiktok.com/?gad_source=1 [https://perma.cc/Z2RD-LUJH] (last visited Apr. 13, 2024).

196 *Id.* at 0:45–0:49.

197 *Id.* at 0:56–1:01.

data in the United States and is managed by United States Data Security (USDS), a U.S. company which operates separately from TikTok and its parent company, ByteDance.[198] TikTok has also worked with USDS to hire an additional 1,000 employees to support this system.[199] TikTok is in the process of appointing an independent board of directors with "strong cybersecurity credentials" to "prevent unauthorized foreign access" to user data.[200] Finally, TikTok is engaged in deleting "historic data" to further protect its users.[201] Its detailed privacy and cybersecurity plan is a clear response to the pending ban or forced sale of platform.[202] Yet, TikTok argues that its data security plan is "the first of its kind" among social media platforms and ensures American users' data is not misused.[203]

In December 2022, TikTok announced the creation of the USDS Trust and Safety Team to "work on compliance, safety strategies, and moderation for content involving U.S. users' private data."[204] As recently as 2023, the corporation opened its first Dedicated Transparency Center in Maryland, "allowing Oracle engineers to begin inspecting and testing TikTok source code."[205] This was likely done to ensure TikTok's code does not

198 *Id.* at 1:02–1:19.

199 *Id.* at 1:19–1:25.

200 *Id.* at 1:26–1:39.

201 *Id.* at 1:42–1:48.

202 *See* sources cited *supra* notes 29–30; *see also* Kevin Freking, Haleluya Hadero & Mary Clare Jalonick, *House Passes a Bill that Could Lead to a TikTok Ban if Chinese Owner Refuses to Sell*, ASSOCIATED PRESS, https://apnews.com/article/tiktok-ban-house-vote-china-national-security-8fa7258fae1a4902d344c9d978d58a37 [https://perma.cc/R45P-ZWQ3] (Mar. 13, 2024, 4:56 PM) (explaining that, per the proposed bill, if the Chinese company ByteDance refuses to sell TikTok and separate from its subsidiary, the bill will ban the social media platform in the United States). The national ban on TikTok is rooted in Congress's belief that the social media company, if its continued ownership is in Chinese hands, poses a "national security threat." *Id.* While a full discussion of the TikTok ban is beyond the scope of this Article, for more information on the ban, see Sarah E. Needleman, *Why TikTok Could Be Banned and What Comes Next*, WALL ST. J. (Mar. 15, 2024, 2:04 PM), https://www.wsj.com/tech/tiktok-ban-explained-7198e7f9 [https://perma.cc/5GR6-7DCW] (explaining the proposed divestiture and potential ramifications of the forced sale).

203 *TikTok U.S. Data Security*, *supra* note 195, at 0:06–0:16, 1:58–2:00.

204 Cormac Keenan, *Strengthening How We Protect and Secure Our Platform in the US*, TIKTOK: U.S. DATA SEC. (Dec. 8, 2022), https://usds.tiktok.com/strengthening-how-we-protect-and-secure-our-platform-in-the-us/ [https://perma.cc/FZ3Q-MPRY].

205 *Dedicated Transparency Center*, TIKTOK: U.S. DATA SEC., https://usds.tiktok.com/dedicated-transparency-center/ [https://perma.cc/L5ZE-EF42] (last visited Sept. 2, 2024).

have any "back doors" that may allow threat actors to illegally access TikTok's cloud storage.

With TikTok's data privacy and cybersecurity practices making headlines, the corporation retooled its data storage and transfer practices in May 2022,[206] and in June 2022 rerouted all new U.S. user traffic to "a secure environment in the Oracle Cloud Infrastructure," rather than to hubs in Virginia and Singapore.[207] While preexisting U.S. data is likely still located in Virginia and Singapore, both places have robust, comprehensive privacy and cybersecurity laws.[208] TikTok follows all state and local laws regarding the management of private data.[209]

Among the types of data TikTok collects, per its website, are personal information (such as name, age, phone number, and profile photo), user-generated content (posts and comments), technical and behavioral information (users' browsing and search history), network information (IP addresses, mobile carrier information), and more.[210]

While it admittedly collects significant amounts of user data, TikTok does *not* collect the following: (1) "Mac addresses, WIFI SSID, IMEI, or SIM serial number[s]"; (2) "Face ID, Fingerprint ID, and facial, body or voice information for the purpose of uniquely identifying a person"; or (3) "[c]ell-based station ID, SMS, email and voicemail content during normal app activities."[211] This data is akin to data collected by other social media platforms like Facebook, Instagram, and Snapchat.[212]

---

206 *Launching U.S. Data Security*, TIKTOK: U.S. DATA SEC., https://usds.tiktok.com/launching-u-s-data-security/ [https://perma.cc/EH7Q-AJF4] (last visited Sept. 2, 2024).

207 *See Routing 100% of All New U.S. User Traffic to the Oracle Cloud Infrastructure*, TIKTOK: U.S. DATA SEC., https://usds.tiktok.com/routing-100-of-all-new-u-s-user-traffic-to-the-oracle-cloud-infrastructure/ [https://perma.cc/KRG9-UJ28] (last visited Sept. 2, 2024).

208 *See* Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to 585 (West 2023) (amended 2024); *see also PDPA Overview*, *supra* note 127 and accompanying text.

209 *See Privacy Policy*, TIKTOK, https://www.tiktok.com/legal/page/us/privacy-policy/en [https://perma.cc/CT9G-ANCZ] (Aug. 19, 2024); *Learn About Data*, TIKTOK, https://www.tiktok.com/privacy/learn-about-data/en [https://perma.cc/4ULU-ME6H] (last visited Apr. 11, 2024) (explaining what types of data TikTok does and does not collect and how that data is used).

210 *Learn About Data*, *supra* note 209.

211 *Id.*

212 *See Privacy Policy*, FACEBOOK: META PRIV. CTR., https://www.facebook.com/privacy/policy/ [https://perma.cc/GDV4-CZ5Z] (last visited Apr. 13, 2024) (covering all Meta platforms, including Facebook and Instagram); *see also Privacy Policy*, SNAP INC.,

Since Snapchat and Meta are both U.S. corporations,[213] their data protection and privacy policies, while scrutinized, have never been threatened by an outright ban.

The U.S. government argues that there is a fundamental threat to national security based on ByteDance's majority ownership stake in the app because "TikTok collects sensitive data on U.S. users and may enable the [Chinese] government to conduct influence operations to shape public opinion."[214] Critics of TikTok allege that it is heavily influenced by ByteDance, which controls what content is shown to U.S. users or "compel[s] TikTok to turn over user data in accordance with various [Chinese] laws that govern cyber and data security."[215] TikTok has wholly denied these allegations,[216] which stem from a 2022 Buzzfeed investigation finding that "China-based employees of ByteDance have repeatedly accessed nonpublic data about US TikTok users."[217] Yet, in this same report, leaked audio caught an external auditor assisting TikTok in shutting off Chinese access to sensitive information like Americans' birthdays and phone numbers, stating, "I feel like with these tools, there's some backdoor to access user data in almost all of them."[218] It was also heard in the leaked audio that "everything is seen in China," and "[i]n another September meeting, a director referred to one Beijing-based engineer as a 'Master Admin' who 'has access to everything.'"[219] While this is certainly concerning, it is worth noting that this discovery came at a time when TikTok was attempting to close any "back doors" to TikTok's U.S. user data[220]

---

https://values.snap.com/privacy/privacy-policy [https://perma.cc/J4E5-KNV8] (last visited Apr. 13, 2024).

213 FACEBOOK, INC. AMENDED & RESTATED CERTIFICATE OF INCORPORATION 2–3 (2021), https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/2024/06/Meta-Platforms-A-R-Certificate-of-Incorporation-06-18-2024.pdf [https://perma.cc/XZM5-CS6Z] (proving that Meta Platforms, Inc. is a Delaware corporation); AMENDED AND RESTATED CERTIFICATE OF INCORPORATION OF SNAP INC. 1 (2017), https://www.sec.gov/Archives/edgar/data/1564408/000119312517029199/d270216dex32.htm [https://perma.cc/EWE9-7ASW] (proving that Snap Inc. is a Delaware corporation).

214 *See* Kristen Busch, *TikTok: Recent Data Privacy and National Security Concerns*, CONG. RSCH. SERV. (Mar. 29, 2023), https://crsreports.congress.gov/product/pdf/IN/IN12131 [https://perma.cc/VV28-DAMZ].

215 *Id.*

216 *Id.*

217 Baker-White, *supra* note 117; *see also* Busch, *supra* note 214.

218 *See* Baker-White, *supra* note 117.

219 *Id.*

220 *Id.*

while the United States still only had a few states with data privacy laws.[221] It is not significant that the discovered breach in their system by Chinese actors happened when only one state had enacted privacy laws to govern the use of private data.[222] True, TikTok has (or *had*) a problem with Chinese access to U.S. user information, but the corporation has taken significant steps to address the issue; in the meantime, no comprehensive federal legislation or clear cross-border data transfer guidance existed.[223]

V. CONFLICT OF LAWS: PROPOSED SOLUTION FOR SAFE AND EFFICIENT DATA STORAGE AND TRANSFERS IN THE AGE OF CLOUD COMPUTING

With data becoming a new global currency for expanding corporations, leaders in technology must work together to find a solution that governments can use to streamline the handling, storage, and transfer of data. If world leaders do not come together to find a solution through treaties, corporations will be left to fill in the gaps.

While it is clear Congress does not have a clear grasp on cross-border data transfer and information governance, the assumption is that TikTok, a corporation owned partially by non-U.S. investors and shareholders, does not have adequate data protection. However, the ownership of TikTok does not necessarily mean that the data is less safe than data held in the United States. In fact, other storage locations, such as Singapore, have had data privacy laws in place long before the United States began passing state-specific privacy laws.[224]

Congressional fear surrounding the handling of data outside the United States is misplaced, as U.S. regulation of data usage has been perpetually behind the curve compared to the EU and other foreign technological centers, which has led to tensions between other world powers (as evidenced by the *Schrems* cases). Even China, with very different views on personal privacy than

---

221 In June 2022, when the audio of the TikTok meeting was leaked, California was the only state to have enacted a comprehensive privacy law. *See* Folks, *supra* note 14.

222 *See id.*

223 It is worth noting that, in 2022, the United States had a data bridge established with the EU and APEC countries; however, as previously discussed, these policies are less than clear. *See supra* Sections IV.A–B.

224 See *supra* Part III, for a discussion on Singapore's data privacy laws.

the United States, passed strict privacy laws years prior to the earliest state privacy law.[225] The attitude Congress currently has toward extraterritorial data policies, other than those originating in the United States, is inappropriate. The United States has attempted on multiple occasions to pass a federal privacy law without success, leaving American citizens' data to be handled in a piecemeal fashion, entirely dependent on whether an individual's state of residence has *any* data privacy protections at all (which the majority of states do not).[226]

A. USMCA as a Basis for a Multilateral Cross-Border Data Transfer Provision

While a discussion of a federal comprehensive privacy law is beyond its scope, this Article proposes a multilateral provision within an existing treaty akin to GDPR to govern cross-border data transfers. Adopting a streamlined process by way of a multinational treaty will create increased consistency and transparency, providing corporations that handle significant amounts of user data, like TikTok, an opportunity to prove that they can adequately follow the rules, without first banning the corporation for alleged misconduct that could leave individuals and business owners without access to their intellectual property.

Rather, implementing a multilateral solution through the signing of a treaty with specific guidelines on cross-border data transfers will encourage compliance and create certainty where there currently are only loose instructions. By using an existing treaty as a basis for these guidelines, the United States can streamline the adoption of new terms and add additional signers to fast-track regulation.

The USMCA would provide an adequate basis for a multilateral agreement for cross-border data transfers. The USMCA is a "21st century, high standard trade agreement [aimed at] supporting mutually beneficial trade resulting in freer markets, fairer trade, and robust economic growth in North

---

225 See *supra* Part III, for a discussion on China's data privacy laws.

226 See *supra* Part III, for a discussion on the current proposed federal privacy law. See *supra* Part I, for a discussion on the piecemeal privacy laws that are currently in place in the United States. As of April 2024, fourteen states have comprehensive privacy laws with varying degrees of protection. *See* Folks, *supra* note 14.

America."[227] The USMCA, which is a replacement for NAFTA,[228] was enacted on July 1, 2020, with the objective to "create[] a more balanced environment for trade, . . . support[] high-paying jobs for Americans, and . . . grow[] the North American economy."[229] Since the USMCA is already in place and would simply require an amendment signed by countries that wish to participate, this would be significantly simpler than starting a new agreement from scratch. To amend the USMCA, the parties would use instructions outlined in the Vienna Convention.[230] Using the Vienna Convention to amend the USMCA would allow for the existing terms to remain in effect and for members to continue the relationship as it currently exists in the agreement, while permitting the addition of new, specific terms for cross-border data transfers.[231] More specifically, Chapter Nineteen, the "Digital Trade" section[232] of the USMCA, already contains the foundation for an amendment to govern extraterritorial data transfers. Chapter Nineteen defines key technical terms such as "computing facility," "information content provider," and "personal information."[233] With additional definitions such as "data controller," "data processor," and other key terms found in privacy laws such as CPRA[234] and GDPR, the definition section can be bolstered to support key privacy terms and educate corporations seeking to engage in data overseas transfers.

Furthermore, adopting standards that comply with *Schrems* guidance and APEC's CPEA could appease foreign entities such as the European Commission and would allow for a greater

---

227 *United States – Mexico – Canada Agreement*, INT'L TRADE ADMIN., https://www.trade.gov/usmca [https://perma.cc/E8KY-EEEK] (last visited Dec. 12, 2023).

228 *See* United States-Mexico-Canada Agreement Implementation Act, Pub. L. No. 116-113, 134 Stat. 11 (2020) (replacing Canada-Mexico-United States: North American Free Trade Agreement, Dec. 17, 1992, 32 I.L.M. 289).

229 *United States – Mexico – Canada Agreement*, *supra* note 227.

230 Vienna Convention on the Law of Treaties art. 39, May 23, 1969, 1155 U.N.T.S. 331.

231 The Vienna Convention provides: "Every State entitled to become a party to the treaty shall also be entitled to become a party to the treaty as amended." *Id.* art. 40. Additionally, "[t]he amending agreement does not bind any State already a party to the treaty which does not become a party to the amending agreement." *Id.*

232 United States-Mexico-Canada Agreement, Nov. 30–Dec. 18, 2018, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf [https://perma.cc/BL7C-F2Q4].

233 *Id.* art. 19.1, at 1–2.

234 CPRA, 2020 Cal. Legis. Serv. Proposition 24 (West) (codified at CAL. CIV. CODE §§ 1798.100—.199.100).

exchange of information between Europe and the United States, as well as other countries. While APEC's CPEA does provide guidance for data transfers, one aspect that would need to be approved if used as a basis for a multilateral cross-border data transfer law would be the creation of an enforcement entity to monitor the transfer of data, similar to what the EU-U.S. Privacy Shield was supposed to do. Since APEC's CPEA is already governed by the U.S. Department of Commerce,[235] creating an enforcement subsidiary within the Department of Commerce that is comprised of privacy, cybersecurity experts, and attorneys to review and approve cross-border transfers would be a significant step toward enforcing a baseline. A recurring criticism of current privacy regimes, including the GDPR, is that enforcement of privacy laws has fallen substantially short of what was anticipated by the public.[236]

Similar to the GDPR, the USMCA could be utilized to govern all member states and constituents of the countries that sign the treaty. Also, Chapter Nineteen could adopt regulations comparable to the CBPRs outlined in APEC's CPEA. While adopting these rules is the first step, the rules would need to be further developed to account for current unclear provisions and emerging issues in privacy and cybersecurity.

Adopting this standard in a multilateral treaty that builds on the current rules in APEC's CPEA leverages existing structures, expanding on what some major players in the world economy have already endorsed. By improving existing standards, it may take less time to draft and adopt legislation that addresses the imminent need for transparent governance.

---

235 *See Global Cross-Border Privacy Rules*, *supra* note 134.

236 *See* Adam Satariano, *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, N.Y. TIMES [hereinafter Satariano, *Europe's Privacy Law*], https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html [https://perma.cc/QM3X-BHXZ] (Apr. 28, 2020); Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CTR. FOR STRATEGIC & INT'L STUD. (Sept. 13, 2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement [https://perma.cc/GZ7H-LMLA]; Anda Bologa, *Fifty Shades of GDPR Privacy: The Good, the Bad, and the Enforcement*, CEPA (Feb. 7, 2023), https://cepa.org/article/fifty-shades-of-gdpr-privacy-the-good-the-bad-and-the-enforcement/ [https://perma.cc/SBH6-DH6V]. *But see* Adam Satariano, *Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules*, N.Y. TIMES (May 22, 2023) [hereinafter Satariano, *Meta Fined*], https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html [https://perma.cc/7PHX-YWJU].

Establishing a specific enforcement body with the power to issue fines or sanctions would also give this solution teeth by encouraging enforcement. While the GDPR has provisions allowing for fines, even after the *Schrems* cases, Facebook has yet to pay a single fine,[237] undermining the GDPR's enforcement capabilities.[238] By leveraging the USMCA as a basis to adopt and enhance APEC's CPEA, the United States can establish a new standard, propelling the United States out of the data privacy stone age into a modern era.

B. Likelihood of Adoption and the Future of Cross-Border Data Governance

While the United States has not previously made data privacy a priority, the massive media attention from the TikTok hearings, coupled with frustration from one of our biggest trade partners, the EU,[239] makes it clear that American lawmakers must act imminently to address major deficiencies in data privacy stemming from current incremental state legislation.[240] With the addition of advanced Artificial Intelligence models to the mix,[241] if the United States does not find and approve a

---

237 *See The Definitive Guide to Schrems II*, *supra* note 175 (explaining that, in *Schrems II*, the CJEU "declared the EU-US Privacy Shield . . . invalid" but did not institute any fines). Facebook has not yet paid a fine in this case because after receiving a landmark fine of 1.2 million Euros, Facebook requested a stay in the case and appealed the fine. Jon Brodkin, *Facebook Hit with Record €1.2 Billion GDPR Fine for Transferring EU Data to US*, ARS TECHNICA (May 22, 2023, 9:36 AM), https://arstechnica.com/tech-policy/2023/05/facebook-ordered-to-pay-e1-2-billion-fine-and-stop-storing-eu-user-data-in-us/ [https://perma.cc/HL88-BR5X].

238 *But see* Satariano, *Meta Fined*, *supra* note 236. This fine came after the *Schrems* decision, which did not result in fines initially:

> The penalty, announced by Ireland's Data Protection Commission, is potentially one of the most consequential in the five years since the European Union enacted the landmark data privacy law known as the General Data Protection Regulation. Regulators said the company failed to comply with a 2020 decision by the European Union's highest court that Facebook data shipped across the Atlantic was not sufficiently protected from American spy agencies.

Id.

239 *U.S.-EU Trade and Economic Relations*, CONG. RSCH. SERV., https://crsreports.congress.gov/product/pdf/IF/IF10931 [https://perma.cc/4BUQ-JNFM] (June 9, 2023).

240 *See* Folks, *supra* note 14.

241 *See* Dr. Mark van Rijmenam, *Privacy in the Age of AI: Risks, Challenges, and Solutions*, DIGITAL SPEAKER (Feb. 17, 2023), https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/ [https://perma.cc/25KQ-MQYD]; *see also* Gai Sher & Ariela Benchlouch, *The Privacy Paradox with AI*, REUTERS (Oct. 31, 2023, 10:15 AM),

solution that addresses the significant lack of guidance in the use of data, private data will be unnecessarily exposed to risk. At the same time, current policies made by ill-informed politicians have led to stifling international business.

Still, the EU displays how government policies are upending the borderless way that data has traditionally moved. As a result of data protection rules, national security laws, and other regulations, companies are increasingly being pushed to store data within the country where it is collected, rather than allowing it to move freely to data centers around the world.[242]

The longer the United States waits to pass comprehensive privacy laws that include clear guidelines and the creation of an enforcement body surrounding cross-border data transfers, the further behind it will be in the figurative "Space Race"[243] of data supremacy. As data-driven technology permeates into everyday life for most Americans,[244] the cost of neglecting to regulate the business of data will become an insurmountable hurdle. Finding a way to open borders for data transfers while still enabling safeguards to protect user data will ultimately improve productivity and boost economic activity.

VI. CONCLUSION

With the monumental surge of data generation in today's society,[245] coupled with a tremendous increase in social media

---

https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/ [https://perma.cc/9FAE-ETFR]. *But see* Thomas H. Davenport & Thomas C. Redman, *How AI Is Improving Data Management*, MIT SLOAN MGMT. REV. (Dec. 20, 2022), https://sloanreview.mit.edu/article/how-ai-is-improving-data-management/ [https://perma.cc/A4TJ-UVP8]; *see also* Scott Clark, *How AI Is Being Used to Protect Customer Privacy*, CMS WIRE (Nov. 4, 2021), https://www.cmswire.com/customer-experience/how-ai-is-being-used-to-protect-customer-privacy/ [https://perma.cc/2VRF-BKXV].

242 *See* Satariano, *Europe's Privacy Law*, *supra* note 236.

243 *What Was the Space Race?*, NAT'L AIR & SPACE MUSEUM (Aug. 23, 2023), https://airandspace.si.edu/stories/editorial/what-was-space-race [https://perma.cc/6Z4G-8QYT] (explaining the origins of the "Space Race" and its significance).

244 *See* Jeffrey Gottfried, *Americans' Social Media Use*, PEW RSCH. CTR. (Jan. 31, 2024), https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/ [https://perma.cc/6G2D-8JXR] (explaining that "YouTube and Facebook are by far the most used online platforms among U.S. adults . . . [and] TikTok's user base has grown since 2021").

245 "According to the latest estimates, 402.74 million terabytes of data are created each day," and around 147 zettabytes of data are expected to be produced in 2024. Duarte, *supra* note 10.

use,[246] it is imperative that the U.S. government takes steps to properly address the lack of clear guidance surrounding cross-border data transfers. As of January 2024, statistics conclude that an astounding 88% of Americans use social media.[247] With the current population of the United States at roughly 335 million,[248] that would mean that roughly 295 million Americans use social media platforms and have their personal data stored by social media corporations like TikTok.[249] The way that corporations use consumer data has changed the international landscape of data use and transfers. "Love, [h]ate or [f]ear it, TikTok [h]as [c]hanged America."[250]

While TikTok is certainly not the first corporation to use massive quantities of consumer data to run its business, its high-profile status, coupled with a contentious congressional hearing that went viral, brought to light the greater issue: where is the data? The proper handling, transfer, and storage of consumer data will continue to be of pivotal importance for corporations and countries alike as the world economy increasingly relies on the use of personal data for a myriad of purposes, such as improving user experience and bettering business models.

By using an already developed and government-approved treaty like the USMCA, the United States can streamline the amendment of a successful multilateral treaty to create guidance in an essential area of international commerce. Amending the USMCA using the Vienna Accords and adding improved data transfer provisions to Chapter Nineteen based on APEC's CPEA can establish certainty in a currently ambiguous space in

246 *See* Gottfried, *supra* note 244.

247 *Number of Social Media Users in the United States from 2020 to 2029*, STATISTICA, https://www.statista.com/statistics/278409/number-of-social-network-users-in-the-united-states/ [https://perma.cc/RZ3K-J54B] (last visited Oct. 9, 2024).

248 *See U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/US/PST045223 [https://perma.cc/JS33-RQSV] (last visited Apr. 14, 2024).

249 According to a recent survey, roughly 170 million Americans use TikTok, which is about half of the U.S. population. Sapna Maheshwari, *Love, Hate or Fear It, TikTok Has Changed America*, N.Y. TIMES (Apr. 19, 2024), https://www.nytimes.com/interactive/2024/04/18/business/media/tiktok-ban-american-culture.html [https://perma.cc/LDQ2-ANPK].

250 *Id.*

international commerce.[251] Having the Department of Commerce act as an enforcement agency would also streamline the adoption of cross-border data provisions, since this government entity is already the governing body for APEC's CPEA.[252]

While APEC's CPEA and governing data privacy rules are a good starting point for a solution, much can be done to improve the guidelines, given that the "accountability" system does not necessarily encourage strict compliance. Giving the Department of Commerce the power to fine entities that violate the data transfer provisions would give these new laws real bite.

Although the EU's GDPR and APEC's CPEA both have flaws and lack much-needed specificity, their principles and rules can give the United States an idea of where to start. Congress must prioritize the adoption of a treaty with clear guidance for entities that engage in cross-border data transfers and must also implement lessons learned from the *Schrems* decisions. Only then can the United States finally exit the digital dark age and propel itself into a new age of data supremacy.

---

251 For a discussion on the "international efforts toward achieving interoperability of privacy and data protection," see Christopher Docksey & Kenneth Propp, *Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective*, OSLO L. REV., Nov. 14, 2023, at 1, 1.

252 *See APEC CPEA*, *supra* note 136.